# directPacket Research

## IPC Platform Setup & Reference Manual

# Contents


*IPC Platform:Setup Guide* ..... 4

*IPC Controller Setup* ..... 5

*IPC Router Setup* ..... 11

*REO:Remote Executive Office* ..... 18

*REO:Soft Switch* ..... 23

*REO:Firmware Check* ..... 23

*REO:System Restore* ..... 24

*STNS:Reference Guide* ..... 25

*Configuration:Community Bridge* ..... 29

*H.323:Video Auto Attendant* ..... 51

*Security:Private Community Keys* ..... 52

*Troubleshooting:STNS Stream* ..... 54

*Troubleshooting:EndPoint Issues* ..... 54

*Troubleshooting:Rescue Mode* ..... 55

*Troubleshooting:Mozilla FireFox Web Browser* ..... 58

The following information needs to be obtained prior to continuing.

Network Settings: IPC Controller

Public Static IP _____

Subnet Mask _____

Default Gateway _____

Network Settings: IPC Router

DHCP

or

Static IP _____

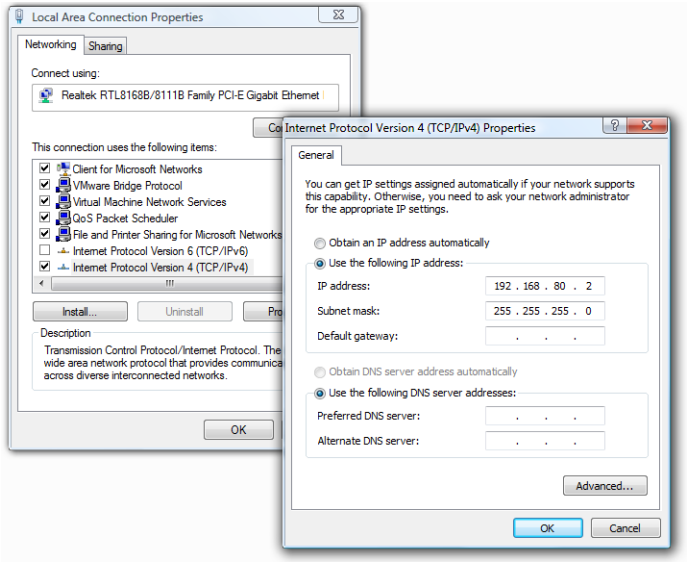
(Remember to exclude from DHCP scope)

Subnet Mask _____

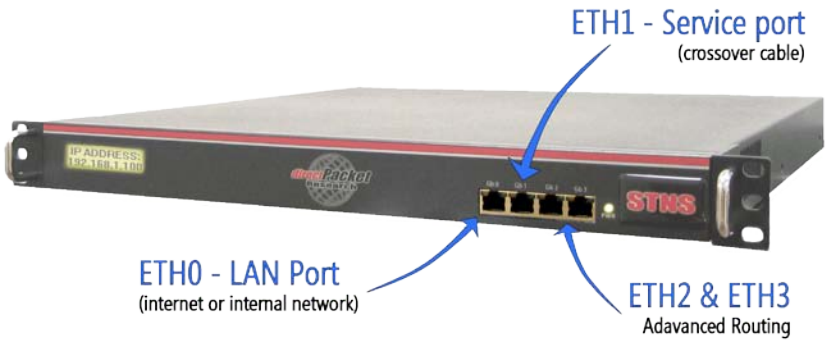
Default Gateway _____

## IPC Controller Setup

Configure your notebook IP address to 192.168.80.2 with a subnet of 255.255.255.0.

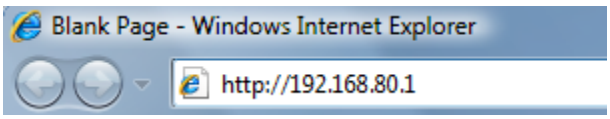

Local Area Connection Properties
Networking
Sharing
Connect using:
Realtek RTL8168B/8111B Family PCI-E Gigabit Ethernet
This connection uses the following items:
Client for Microsoft Networks
VMware Bridge Protocol
Virtual Machine Network Services
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Install...
Uninstall
Description
Transmission Control Protocol/Internet Protocol. The
wide area network protocol that provides communica
across diverse interconnected networks.
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 80 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Connect a notebook via the service port on the IPC Controller using a crossover cable.



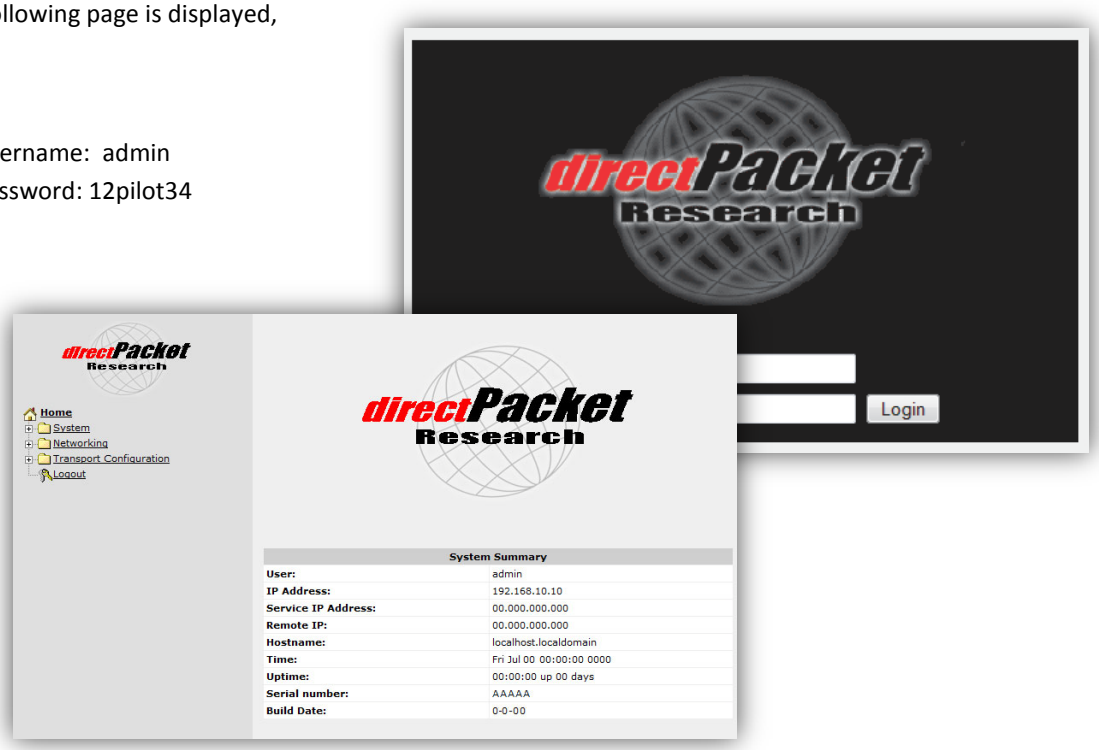

Open the URL: **http://192.168.80.1**

This URL is only accessible from this port.



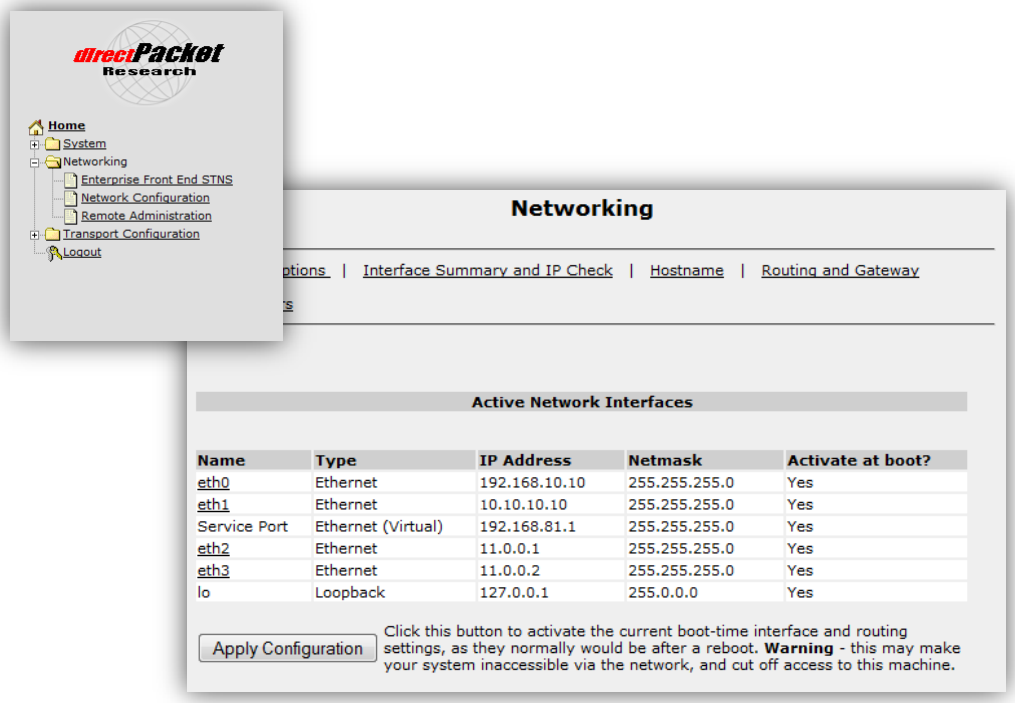
Once the following page is displayed, login using:

Username: admin
Password: 12pilot34



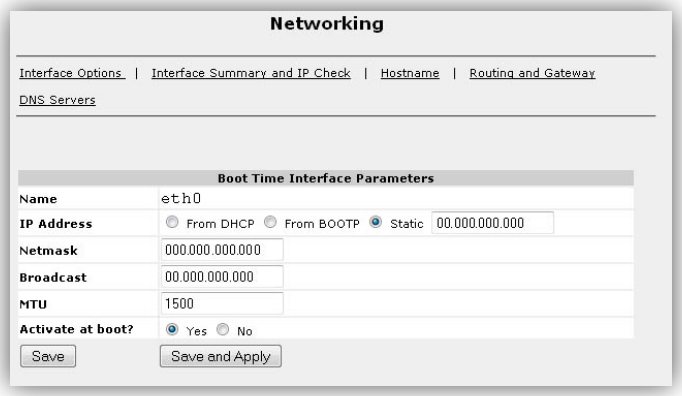

Once successfully logged in, you will see the page displayed above.

First, we will configure the network ports. Select **Networking** and then select **Network Configuration**.

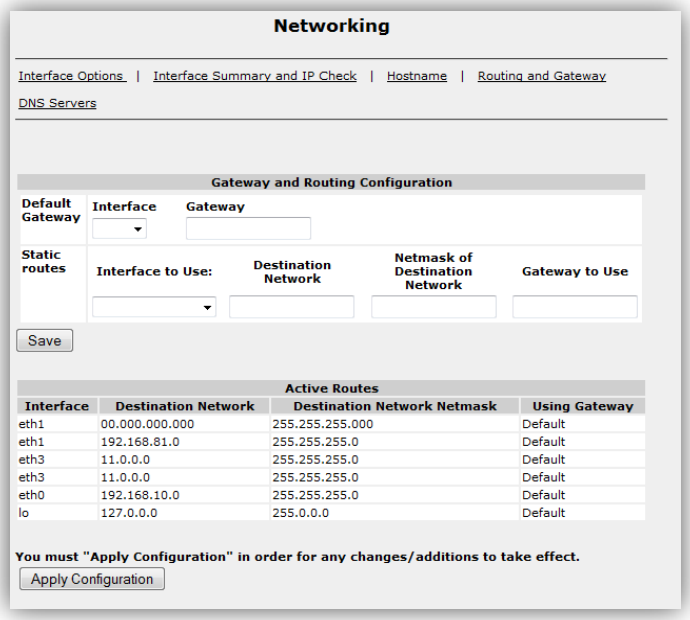

directPacket
Research
Home
System
Networking
Enterprise Front End STNS
Network Configuration
Remote Administration
Transport Configuration
Logout
Networking
Interface Summary and IP Check | Hostname | Routing and Gateway
Active Network Interfaces
Name Type IP Address Netmask Activate at boot?
eth0 Ethernet 192.168.10.10 255.255.255.0 Yes
eth1 Ethernet 10.10.10.10 255.255.255.0 Yes
Service Port Ethernet (Virtual) 192.168.81.1 255.255.255.0 Yes
eth2 Ethernet 11.0.0.1 255.255.255.0 Yes
eth3 Ethernet 11.0.0.2 255.255.255.0 Yes
lo Loopback 127.0.0.1 255.0.0.0 Yes
Apply Configuration
Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to this machine.

Select eth0.

Set the **IP address**, **Netmask**, **Broadcast** and **MTU** settings of your choice. If there isn't a preferred MTU setting, use 1500. Once completed, click **Save**.

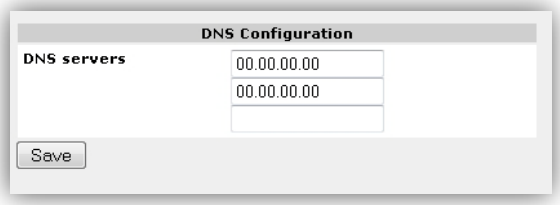



Select the **Routing and Gateway** link.

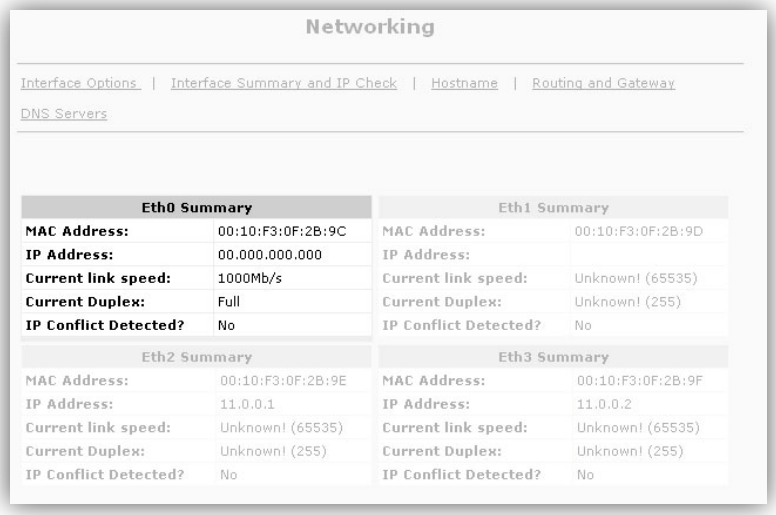



Click the Interface drop down and choose eth0 and specify the Gateway settings. Click **Save**.

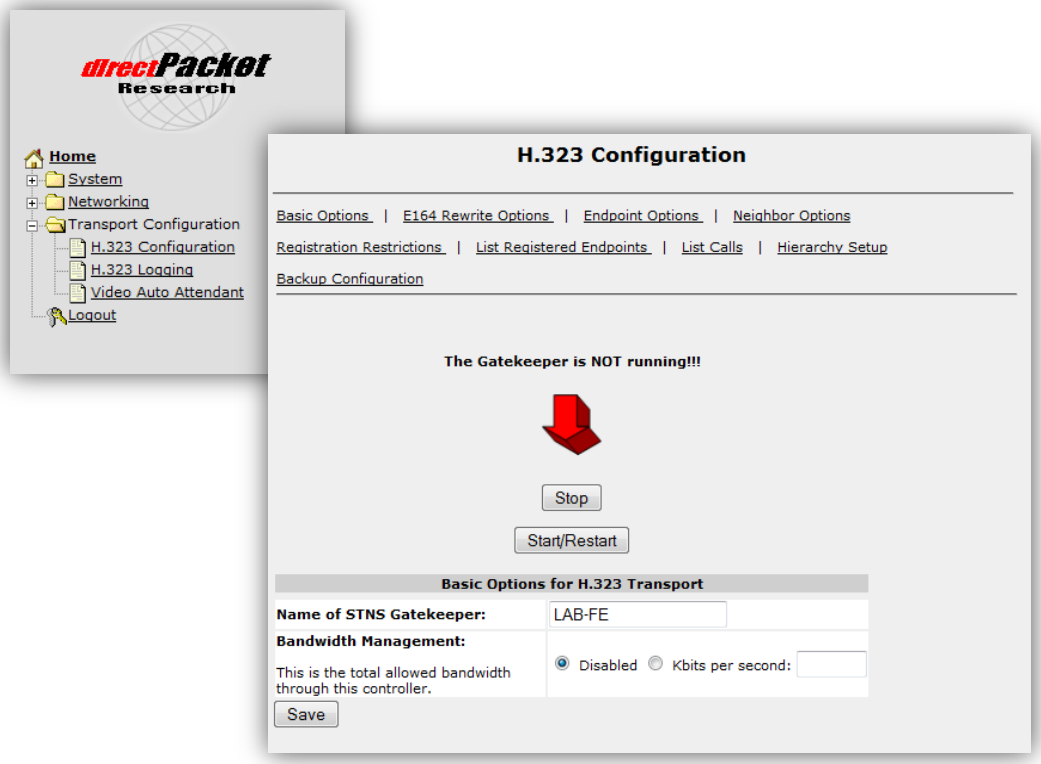
Select **DNS Servers** and enter in the appropriate DNS servers you have received from your network administrator.
Select the Interface Options link and click **Save** and then click on **Apply Configuration**.



Under Interface Summary and IP Check, verify the Speed and Duplex are set to 100 or 1000 Mbits Full for eth0 and that there is no IP conflicts detected. If there is an IP conflict, please revisit the IP configuration and verify your network settings.



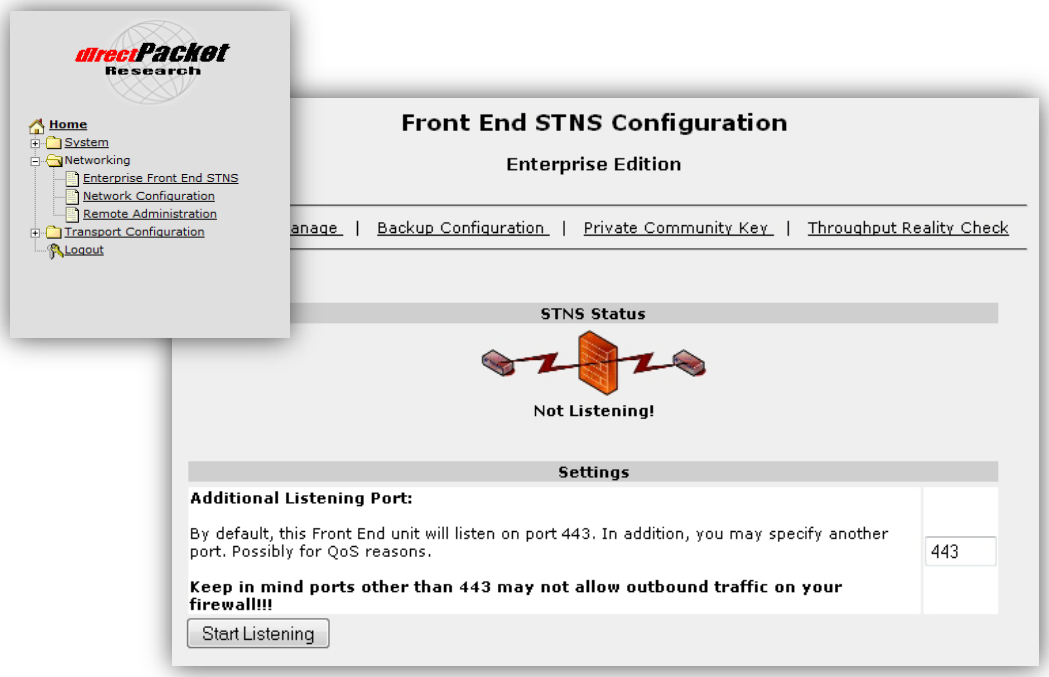

In the left hand navigation pane, choose**: Transport Configuration** and then **H.323 Configuration**.




Change the Gatekeeper to a unique name. For example: FEGate1, FrontEndGK1, FEGK1

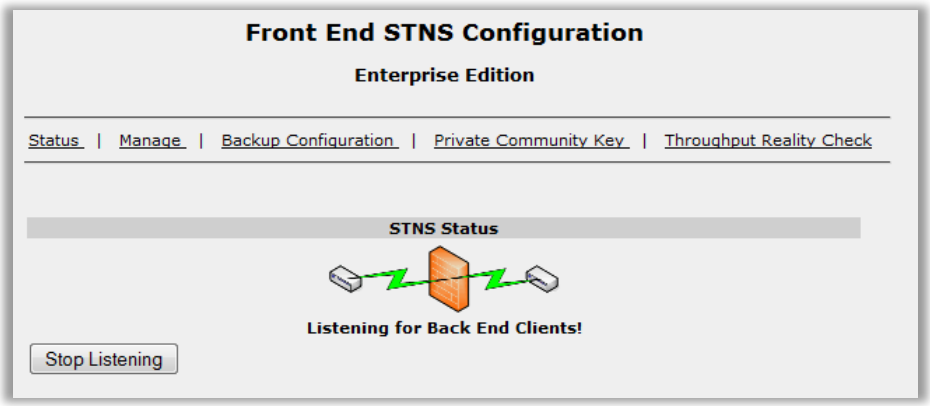
Click **Save** and then **Save Changes Only**.

Using the left hand navigation pane, navigate to Networking, Enterprise Front End.


directPacket Research
Home
System
Networking
Enterprise Front End STNS
Network Configuration
Remote Administration
Transport Configuration
Logout
Front End STNS Configuration
Enterprise Edition
anage | Backup Configuration | Private Community Key | Throughput Reality Check
STNS Status
Not Listening!
Settings
Additional Listening Port:
By default, this Front End unit will listen on port 443. In addition, you may specify another port. Possibly for QoS reasons.
443
Keep in mind ports other than 443 may not allow outbound traffic on your firewall!!!
Start Listening

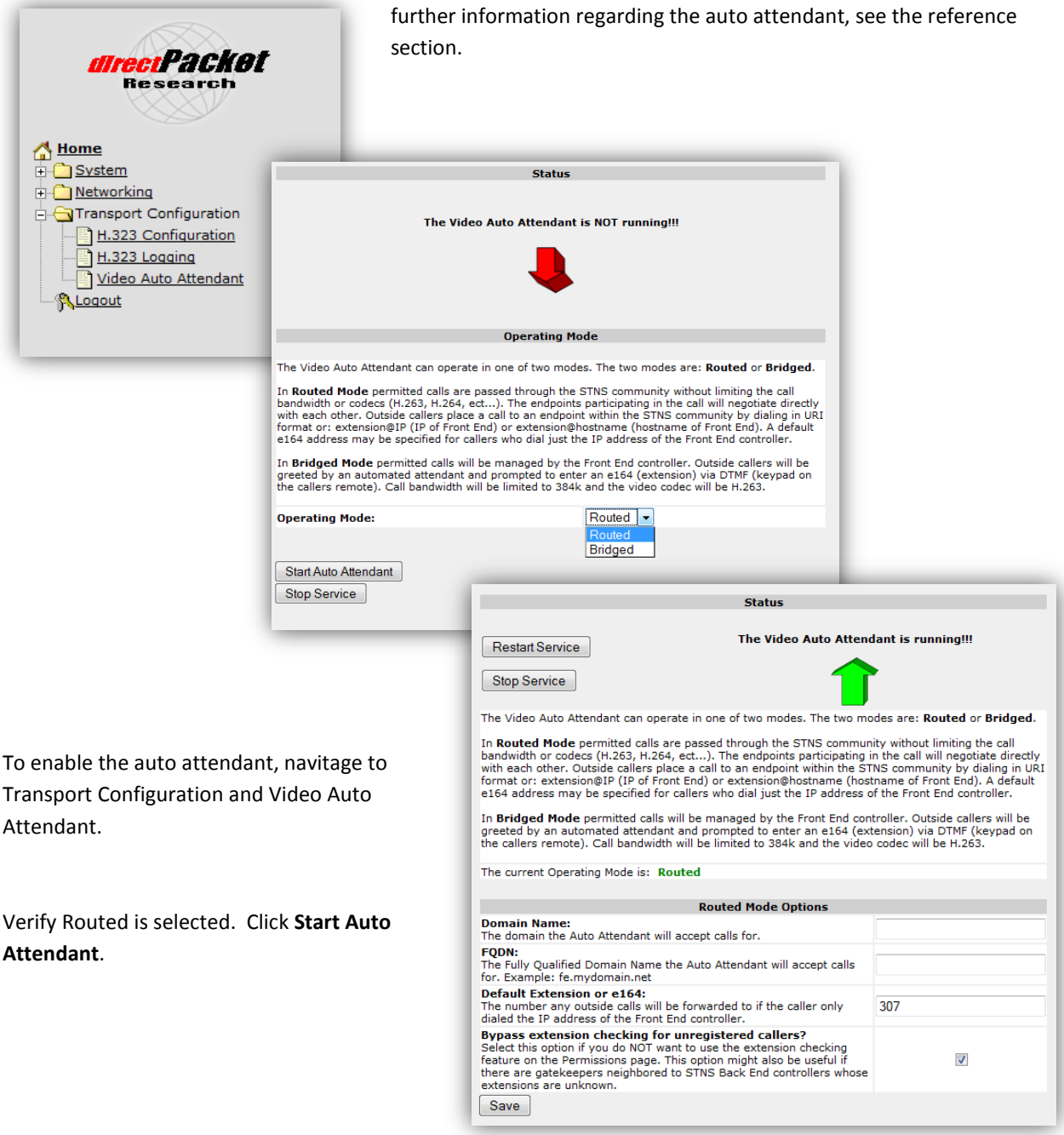
Using the default port 443, press the **Start Listening** button. The Front End startup process can take up to two minutes to complete. Watch the browser's progress indicator and do not navigate away from this page.

Once the process is complete, the user will be redirected to the status page shown below.


Front End STNS Configuration
Enterprise Edition
Status | Manage | Backup Configuration | Private Community Key | Throughput Reality Check
STNS Status
Listening for Back End Clients!
Stop Listening

At this time, the IPC-Controller is listening for IPC-Router and REO connections.

Next, the IPC Controller will be set up in a routed mode for all calls. For further information regarding the auto attendant, see the reference section.


directPacket Research
Home
System
Networking
Transport Configuration
H.323 Configuration
H.323 Logging
Video Auto Attendant
Logout
Status
The Video Auto Attendant is NOT running!!!
Operating Mode
The Video Auto Attendant can operate in one of two modes. The two modes are: Routed or Bridged.
In Routed Mode permitted calls are passed through the STNS community without limiting the call bandwidth or codecs (H.263, H.264, ect...). The endpoints participating in the call will negotiate directly with each other. Outside callers place a call to an endpoint within the STNS community by dialing in URI format or: extension@IP (IP of Front End) or extension@hostname (hostname of Front End). A default e164 address may be specified for callers who dial just the IP address of the Front End controller.
In Bridged Mode permitted calls will be managed by the Front End controller. Outside callers will be greeted by an automated attendant and prompted to enter an e164 (extension) via DTMF (keypad on the callers remote). Call bandwidth will be limited to 384k and the video codec will be H.263.
Operating Mode:
Routed
Routed
Bridged
Start Auto Attendant
Stop Service
Status
Restart Service
Stop Service
The Video Auto Attendant is running!!!
The Video Auto Attendant can operate in one of two modes. The two modes are: Routed or Bridged.
In Routed Mode permitted calls are passed through the STNS community without limiting the call bandwidth or codecs (H.263, H.264, ect...). The endpoints participating in the call will negotiate directly with each other. Outside callers place a call to an endpoint within the STNS community by dialing in URI format or: extension@IP (IP of Front End) or extension@hostname (hostname of Front End). A default e164 address may be specified for callers who dial just the IP address of the Front End controller.
In Bridged Mode permitted calls will be managed by the Front End controller. Outside callers will be greeted by an automated attendant and prompted to enter an e164 (extension) via DTMF (keypad on the callers remote). Call bandwidth will be limited to 384k and the video codec will be H.263.
The current Operating Mode is: Routed
Routed Mode Options
Domain Name:
The domain the Auto Attendant will accept calls for.
FQDN:
The Fully Qualified Domain Name the Auto Attendant will accept calls for. Example: fe.mydomain.net
Default Extension or e164:
The number any outside calls will be forwarded to if the caller only dialed the IP address of the Front End controller.
307
Bypass extension checking for unregistered callers?
Select this option if you do NOT want to use the extension checking feature on the Permissions page. This option might also be useful if there are gatekeepers neighbored to STNS Back End controllers whose extensions are unknown.
Save

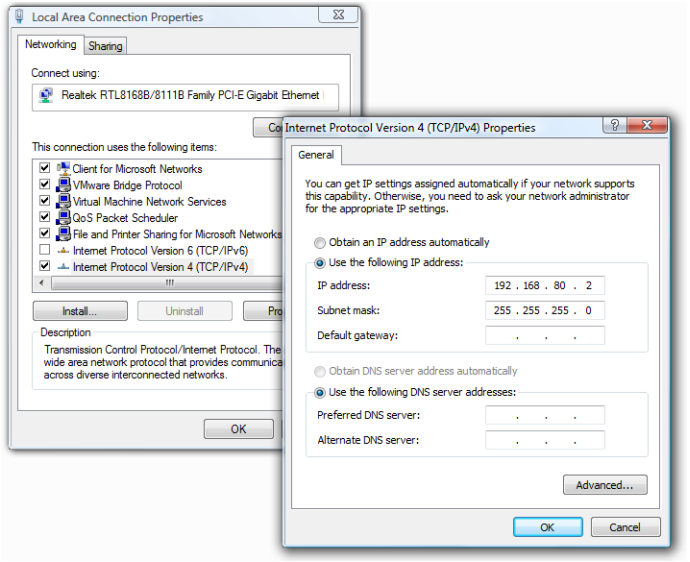
To enable the auto attendant, navitage to Transport Configuration and Video Auto Attendant.

Verify Routed is selected. Click **Start Auto Attendant**.

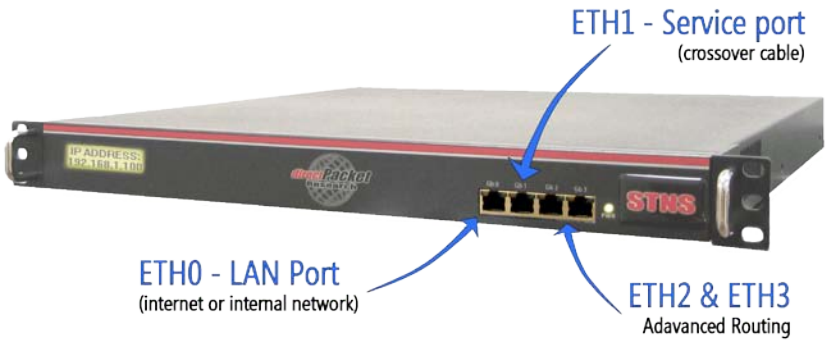
This concludes the IPC Controller configuration portions. Proceed to IPC Router setup.

# IPC Router Setup

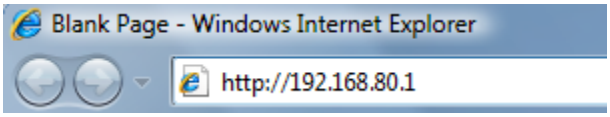
Just like the IPC Controller, configure your notebook IP address to 192.168.80.2 with a subnet of 255.255.255.0.


Local Area Connection Properties
Networking
Sharing
Connect using:
Realtek RTL8168B/8111B Family PCI-E Gigabit Ethernet
This connection uses the following items:
Client for Microsoft Networks
VMware Bridge Protocol
Virtual Machine Network Services
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Install...
Uninstall
Description
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address: 192 . 168 . 80 . 2
Subnet mask: 255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

Connect a notebook via the service port on the  IPC Router using a crossover cable.

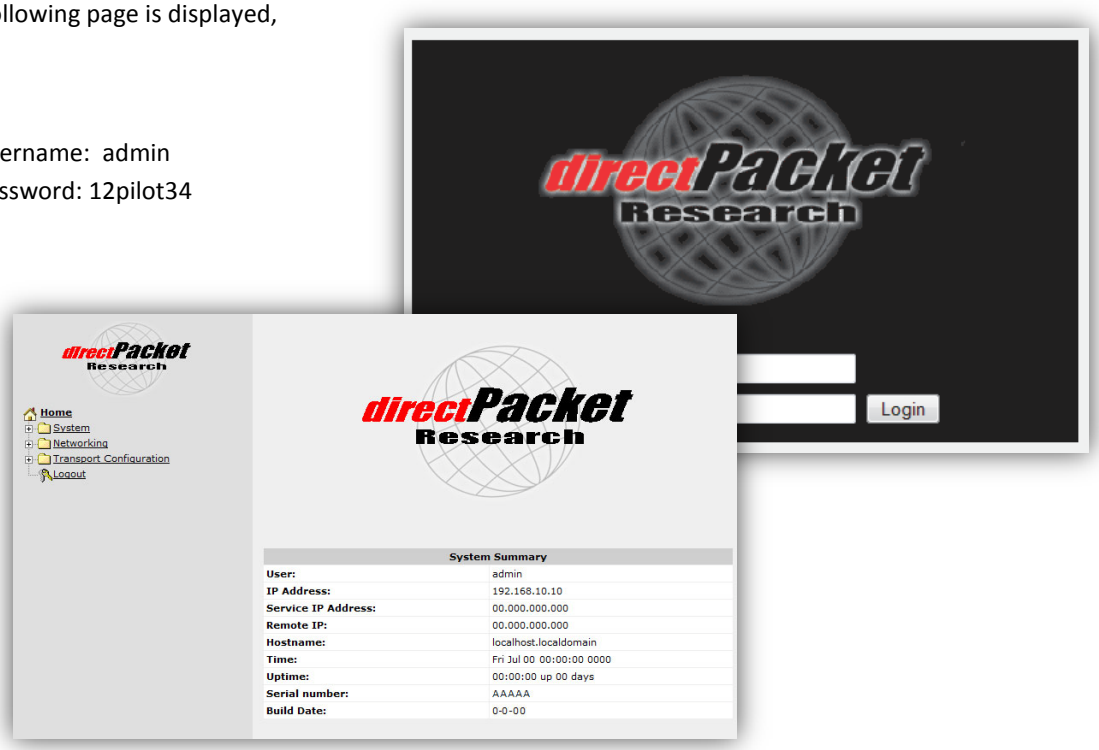



Open the URL:  **http://192.168.80.1**
This URL is only accessible from this port.



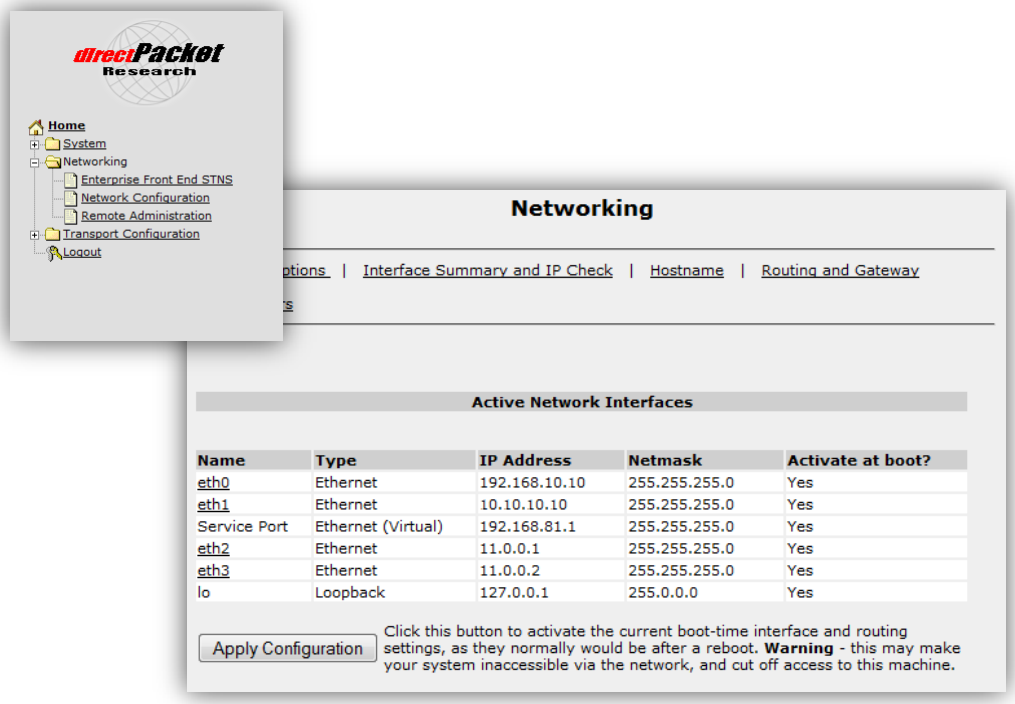
Once the following page is displayed, login using:

Username: admin
Password: 12pilot34



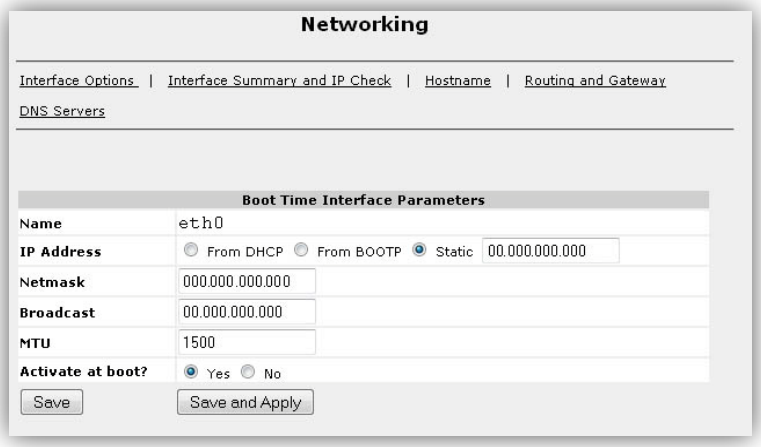

Once successfully logged in, you will see the page displayed above.

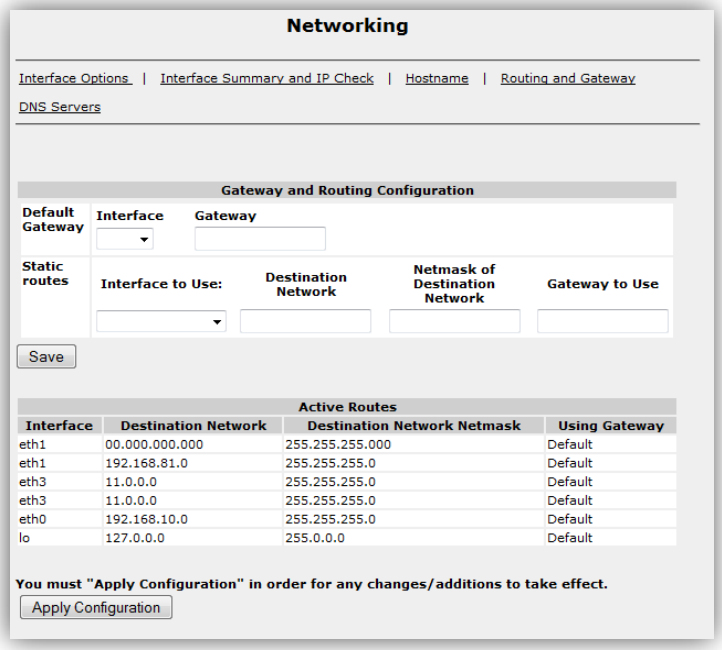
First, we will configure the network ports. Select **Networking** and then select **Network Configuration**.


directPacket
Research
Home
System
Networking
Enterprise Front End STNS
Network Configuration
Remote Administration
Transport Configuration
Logout
Networking
Interface Summary and IP Check | Hostname | Routing and Gateway
Active Network Interfaces
Name Type IP Address Netmask Activate at boot?
eth0 Ethernet 192.168.10.10 255.255.255.0 Yes
eth1 Ethernet 10.10.10.10 255.255.255.0 Yes
Service Port Ethernet (Virtual) 192.168.81.1 255.255.255.0 Yes
eth2 Ethernet 11.0.0.1 255.255.255.0 Yes
eth3 Ethernet 11.0.0.2 255.255.255.0 Yes
lo Loopback 127.0.0.1 255.0.0.0 Yes
Apply Configuration
Click this button to activate the current boot-time interface and routing settings, as they normally would be after a reboot. Warning - this may make your system inaccessible via the network, and cut off access to this machine.

Select eth0

Set the **IP address**, **Netmask**, **Broadcast** and **MTU** settings of your choice. If there isn't a preferred MTU setting, use 1500. Once completed, click **Save**.



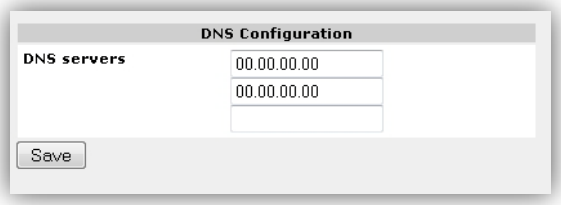




Select the **Routing and Gateway** link.

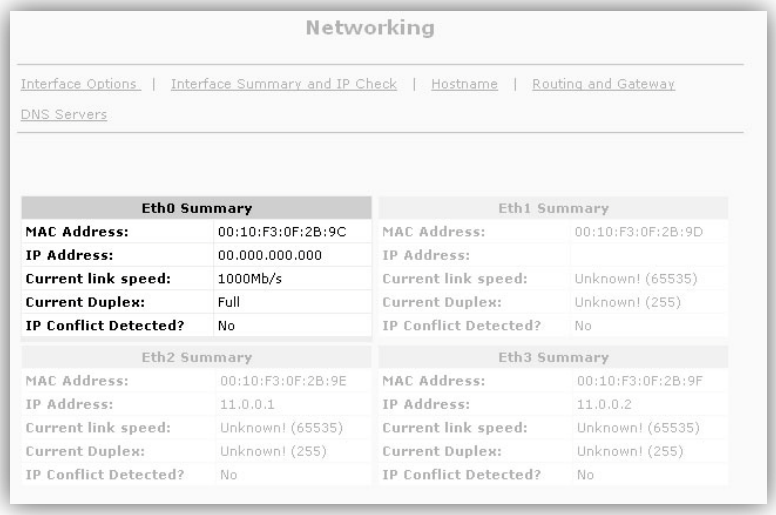
Click the Interface drop down and choose eth0 and specify the Gateway settings. Click **Save** and then click **Apply Configuration**.

Select **DNS Servers** and enter in the appropriate DNS servers you have received from your network administrator.

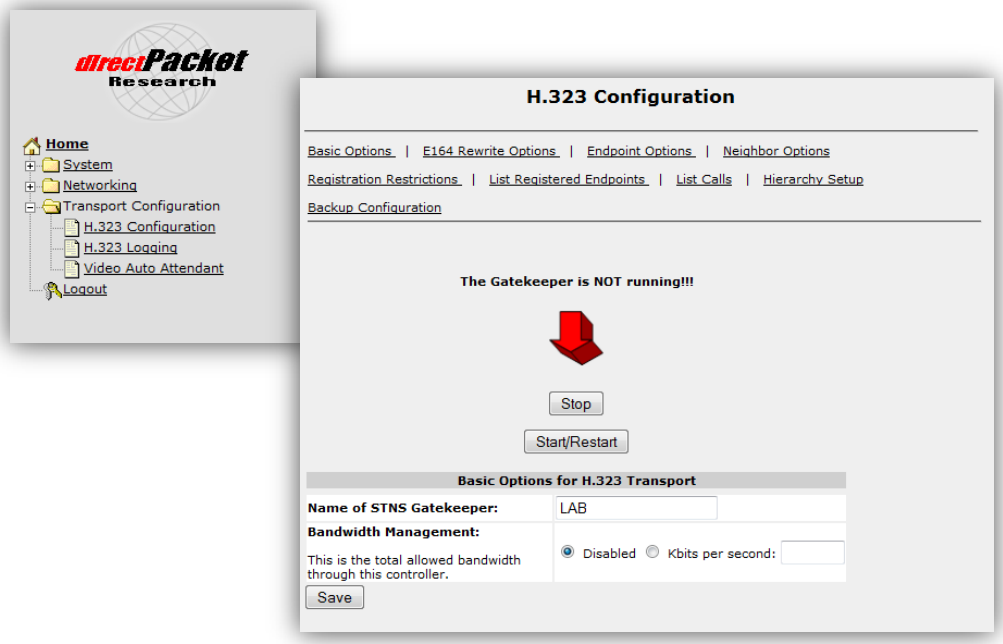
Select the Interface Options link and click **Save** and then click on **Apply Configuration**.



Under Interface Summary and IP Check, verify the Speed and Duplex are set to 100 or 1000 Mbits Full for eth0. Verify there is no IP conflict detected.




In the left hand navigation pane, choose**: Transport Configuration** and then **H.323 Configuration**.

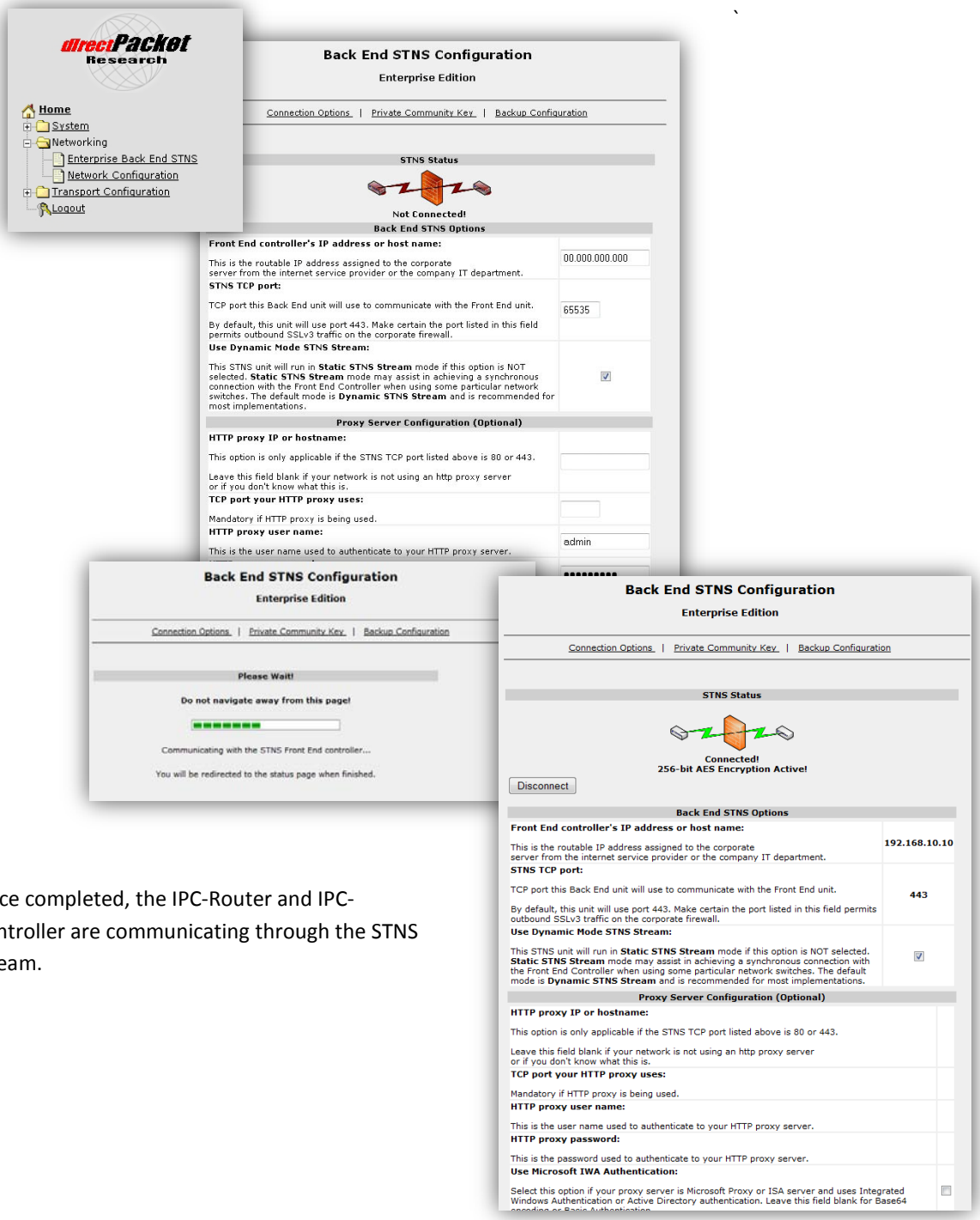



Change the Gatekeeper to a unique name. For example: FEGate1, FrontEndGK1, FEGK1

Click **Save** and then **Save Changes Only**. We will return to this page to complete the configuration after the STNS link is established.

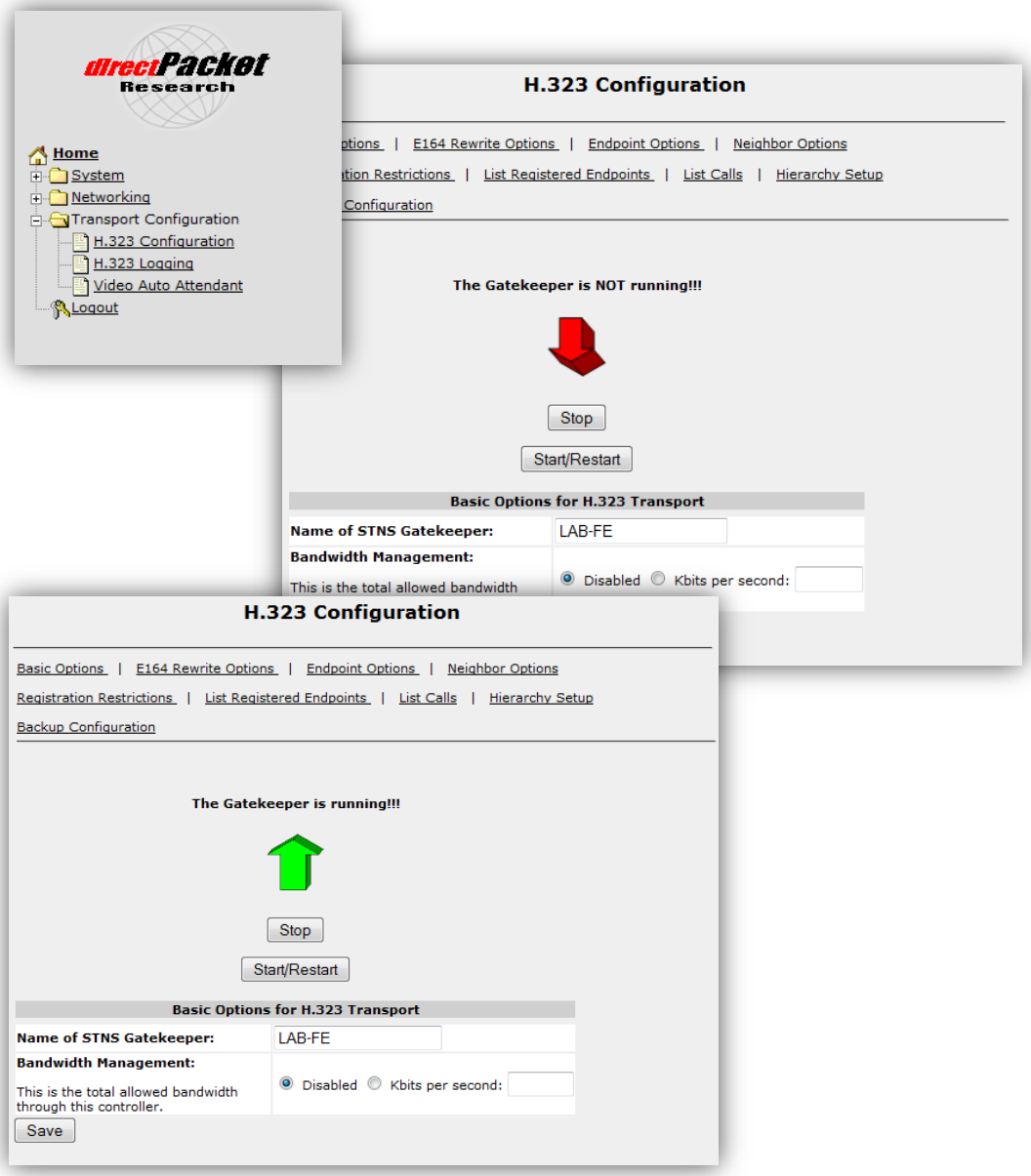
Navigate to **Networking** and **Enterprise Back End STNS**. Enter the IP Address or host name of the IPC Controller.

If you are using a proxy server, enter the address and TCP port of the HTTP proxy server and authentication information if necessary. Otherwise, leave them blank. Scroll to the bottom of the page and click Connect. Watch your browser, and do not navigate away from this page. This process can take up to 120 seconds.

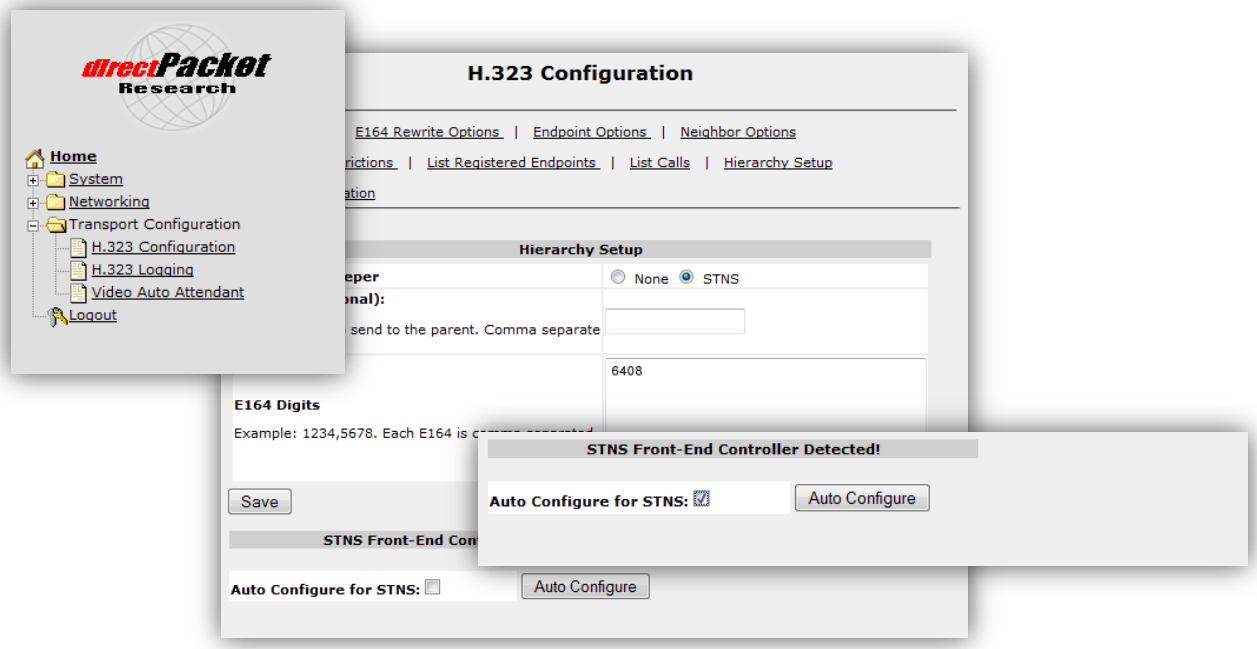



Once completed, the IPC-Router and IPC-Controller are communicating through the STNS stream.

Navigate to **Transport Configuration**, **H.323 Configuration**. Click on **Save**, then **Start/Restart Gatekeeper**. At this point, the gatekeeper will restart and the endpoints will register to the IPC-Router.



Next, we need to list which endpoints will be traversing the firewall.
Navigate to **Transport Configuration**, **H.323 Configuration**, and **Hierarchy Setup**.

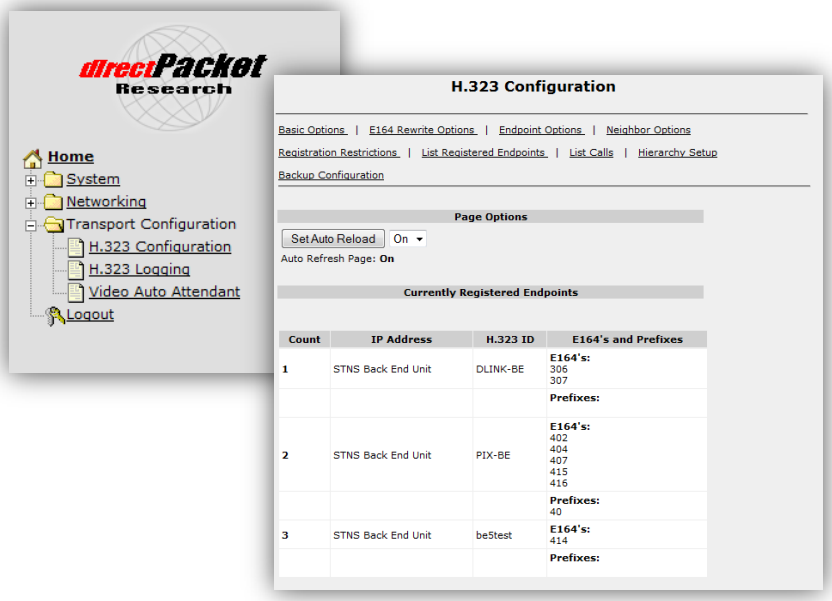



Place a checkmark in the **Auto Configure for STNS** and click **Auto Configure**. The E164's for all registered endpoints will show up in the E164 digits field. Remove any E164 which you do NOT wish to traverse the firewall. Prefixes can be added at this time if desired. Click **Save** and then **Start/Restart Gatekeeper**.

Next, verify your endpoints by navigating to **Transport Configuration**, **H.323 Configuration**, and **List Endpoints**.

Verify the endpoints on the IPC-Controller. Each endpoint will be registered under the associated IPC-Router.

This concludes the IPC-Controller and IPC-Router configuration scenario. You are ready to make calls. If you have any troubles, see the troubleshooting guide at the end of this manual.



# REO:Remote Executive Office

The REO appliance is smaller IPC Router meant to traverse firewalls with roaming endpoints in the office, hotels, or other remote locations. All the features from three product generations of REOs are included in this manual. If there are any questions for compatibility or capability, please inquire with your DirectPacket reseller.

The REO, is different from the Enterprise version in the following ways:

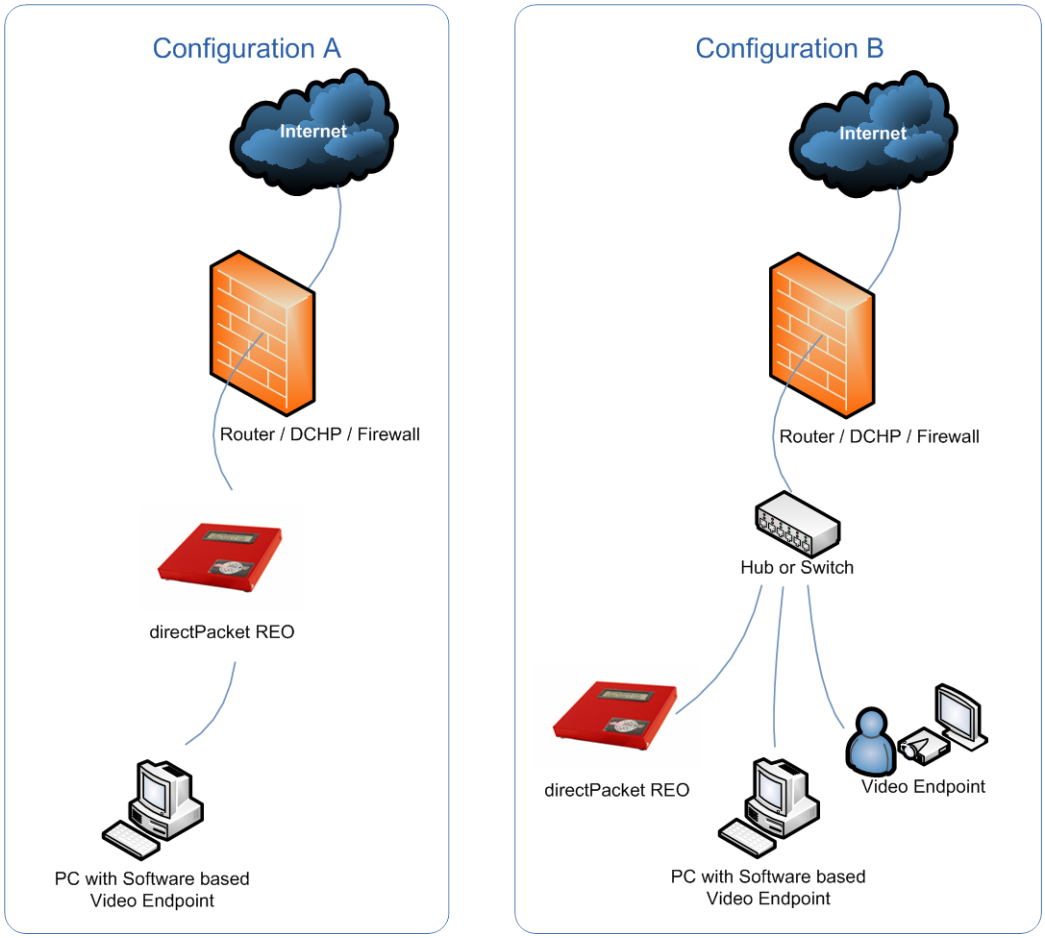
- Only a single endpoint is supported.
- There is no H.323 module installed.
- The REO IPC Router module is a wizard that only asks a few questions.

The end user will need to have obtained the following information from their IT department prior to continuing:

IP or hostname of IPC-Controller _____

Your assigned E164 Address _____

The REO is used in one of two different configurations.




If using configuration A, follow these steps:

1. Connect the LAN Ethernet cable to the REO.
2. Connect your workstation to REO's PC/EP network interface via the supplied crossover cable.
3. Verify your workstation is set to use DHCP server.
4. Power the REO unit on and wait until the LCD screen displays an IP address.
5. Turn on your workstation.
6. Check your IP address. It should be either 192.168.80.2 or 192.168.80.3. If it is not, renew your ip address.
7. Open a web browser and navigate to http://192.168.80.1

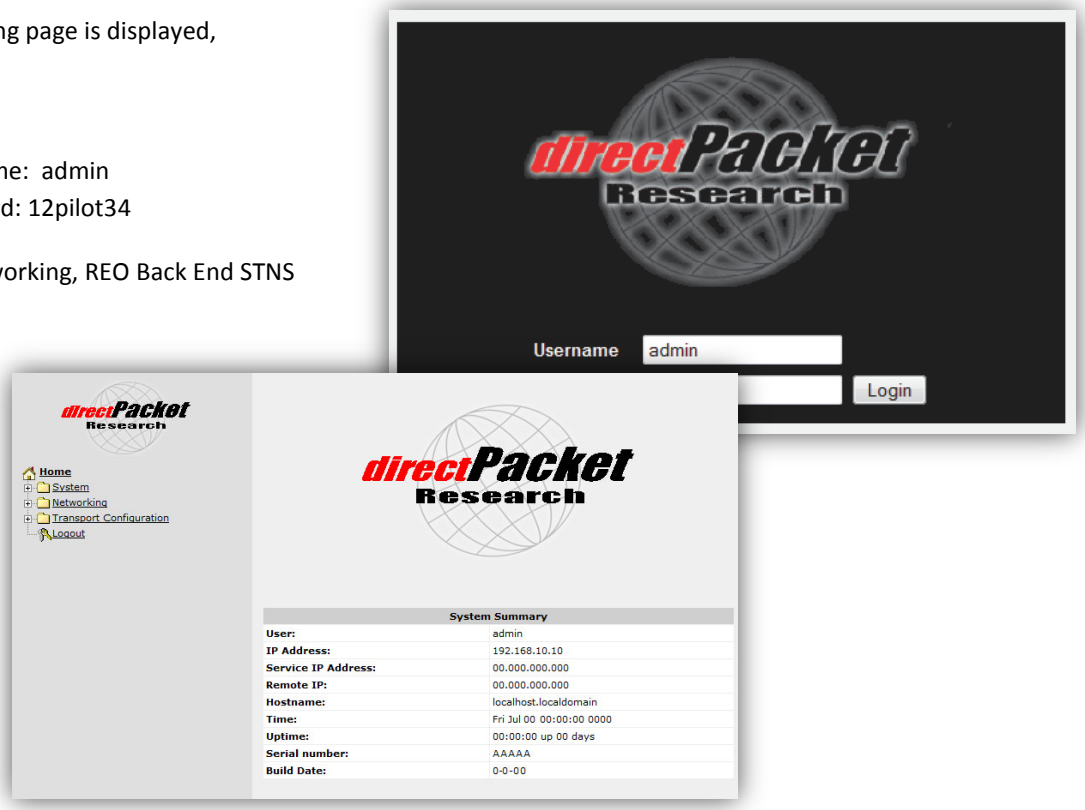
If using Configuration B follow these steps:

1. Connect the LAN Ethernet cable to the REO.
2. Power the REO unit on and wait until the LCD screen displays an IP address
3. Open a web browser and navigate to **http://*<IP Address displayed on the LCD screen>***
4. Proceed to step 1 on the next page.

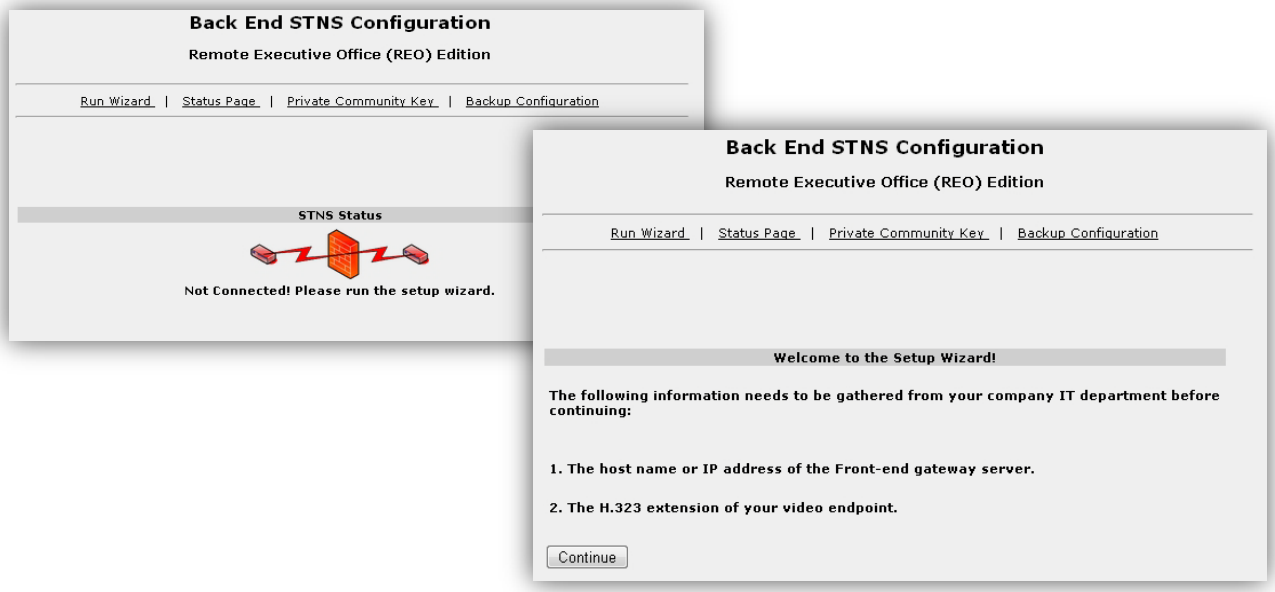
Once the following page is displayed, login using:

Username: admin
Password: 12pilot34

Navigate to Networking, REO Back End STNS




The following screens will be displayed. Click Run Wizard and Continue.

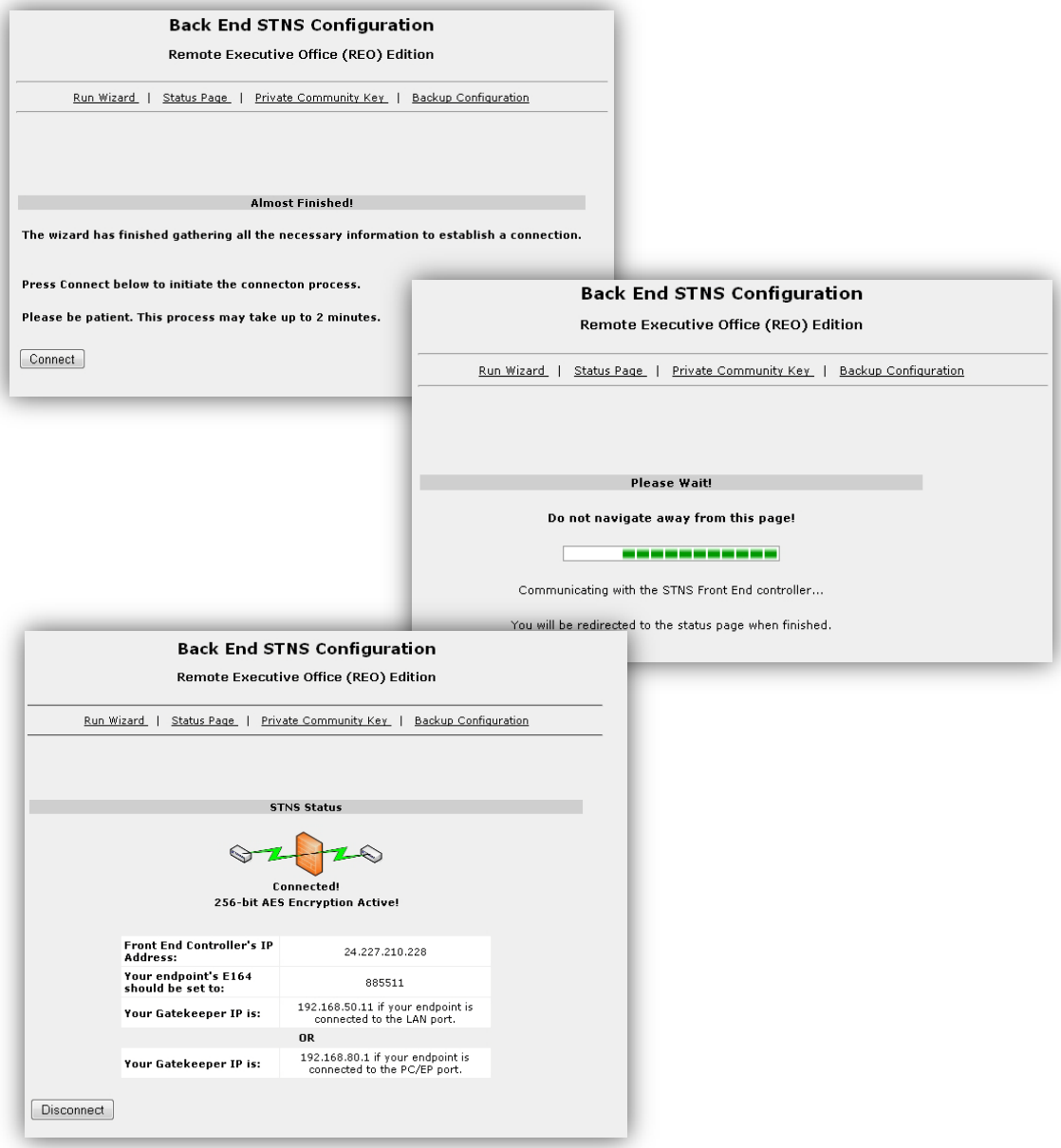

Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
STNS Status
Not Connected! Please run the setup wizard.
Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
Welcome to the Setup Wizard!
The following information needs to be gathered from your company IT department before continuing:
1. The host name or IP address of the Front-end gateway server.
2. The H.323 extension of your video endpoint.
Continue

The wizard will walk you through four simple steps to set up the REO to a Front End controller.

Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
Step: 1
Enter the Front-end gateway server's host name or IP address:
This is the routable IP address assigned to the corporate server from the internet service provider or the company IT department.
0.0.0.0
Continue
Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
Step: 2
Enter the H.323 extension assigned to you from your company IT department.
This will be the extension people from within your company will use to call you.
885511
Continue
Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
Step: 3
Please enter the first initial from your first name and your last name.
EXAMPLE: jsmith.
Reo
Continue

After following the directions above for the specific network configuration, the wizard takes you through a few easy steps.

Enter in  the IP address of the Front End controller.
Enter in your E164 address.
Enter a name for the system such as your name.
Connect to the Front End controller.


Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
Almost Finished!
The wizard has finished gathering all the necessary information to establish a connection.
Press Connect below to initiate the connecton process.
Please be patient. This process may take up to 2 minutes.
Connect
Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
Please Wait!
Do not navigate away from this page!
Communicating with the STNS Front End controller...
You will be redirected to the status page when finished.
Back End STNS Configuration
Remote Executive Office (REO) Edition
Run Wizard | Status Page | Private Community Key | Backup Configuration
STNS Status
Connected!
256-bit AES Encryption Active!
Front End Controller's IP Address: 24.227.210.228
Your endpoint's E164 should be set to: 885511
Your Gatekeeper IP is: 192.168.50.11 if your endpoint is connected to the LAN port.
OR
Your Gatekeeper IP is: 192.168.80.1 if your endpoint is connected to the PC/EP port.
Disconnect

Set up is complete.  You are now ready to make calls through the endpoint.

## REO:Soft Switch

The latest REO includes a soft switch power button.

**Press the power button once**, without holding it down, the system will shut down and display the following message on the LCD:

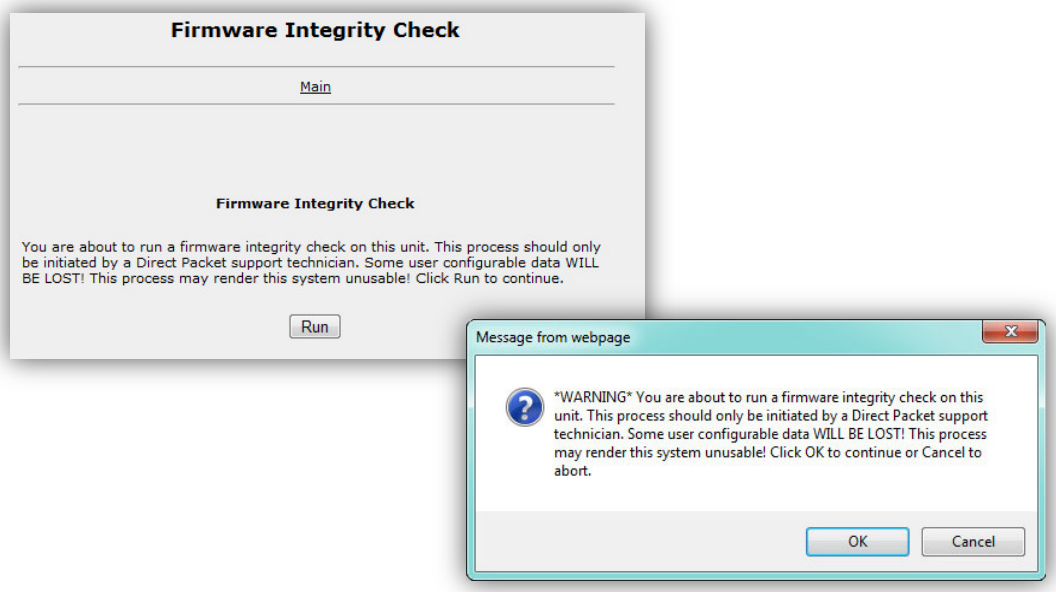
**"Please wait…"**
**"Shutting down! " ***

The system will state ** **Wait 20 seconds**** before shutting down on its own. Once shutdown it is safe to unplug or restart the system.

**Press and hold the power button down** will force a shutdown of the system without properly shutting down the services running on the system. This is not recommended.

## REO:Firmware Check

Current systems are included with a firmware integrity check. Previously shipped systems can have this option added through updates with a Direct Packet support technician. This option will attempt to correct any file corruption issues if they occur. Performing this option will restart the system once completed. All system settings will be preserved during this process.

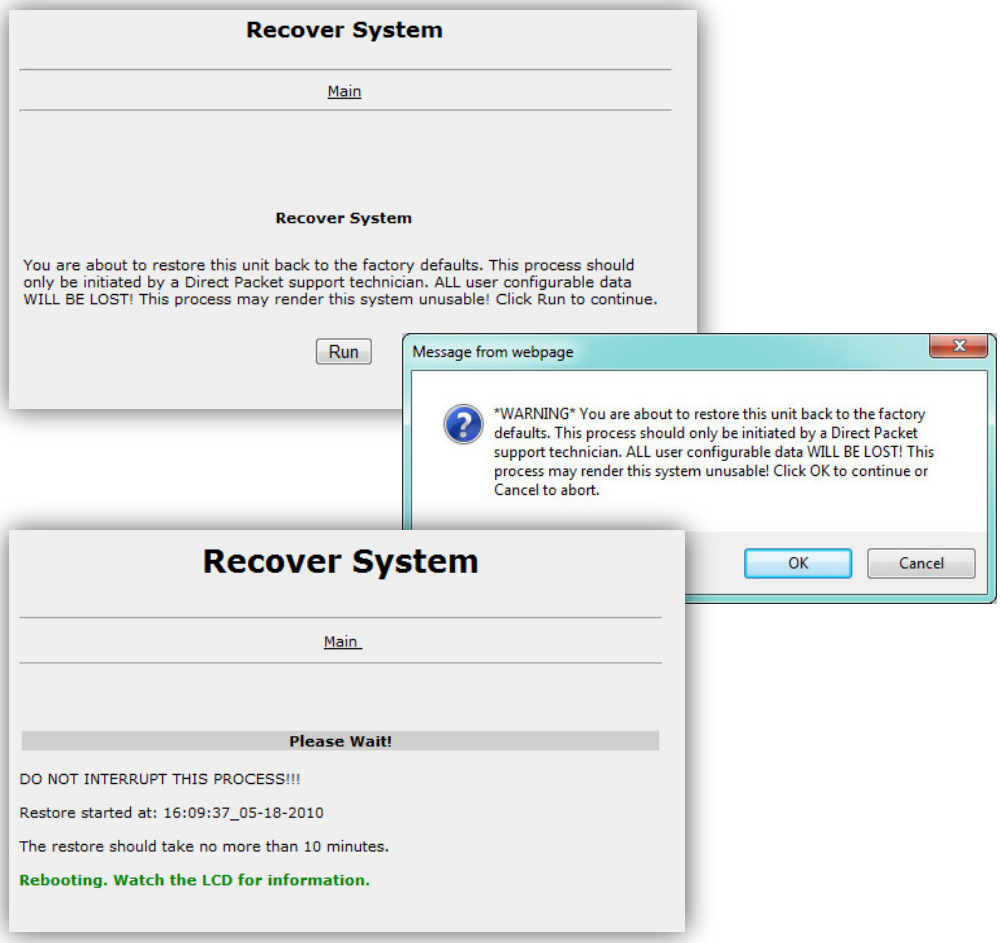

Firmware Integrity Check
Main
Firmware Integrity Check
You are about to run a firmware integrity check on this unit. This process should only be initiated by a Direct Packet support technician. Some user configurable data WILL BE LOST! This process may render this system unusable! Click Run to continue.
Run
Message from webpage
*WARNING* You are about to run a firmware integrity check on this unit. This process should only be initiated by a Direct Packet support technician. Some user configurable data WILL BE LOST! This process may render this system unusable! Click OK to continue or Cancel to abort.
OK
Cancel

# REO:System Restore

With the latest REO release, there is a system restore option. This option will restore all settings and modules back to their original shipped configurations. If any updated modules were installed months or years after receiving the REO unit, they will need to be updated again with the assistance of a Direct Packet technician.

To access the System Restore option, you must use the Rescue Mode by configuring your address to: 192.168.81.2 and logging into to http://192.168.81.1:911.

Once the option is clicked, the system will restart and the LCD screen will say: **"Restoring System Please Wait"** This process will take no more than 10 minutes. The LCD screen will not change until it is completed. Once completed, the system will restart itself and Direct Packet Research will appear on the screen. Then IP Address will be displayed where you can connect to.


Recover System
Main
Recover System
You are about to restore this unit back to the factory defaults. This process should only be initiated by a Direct Packet support technician. ALL user configurable data WILL BE LOST! This process may render this system unusable! Click Run to continue.
Run
Message from webpage
*WARNING* You are about to restore this unit back to the factory defaults. This process should only be initiated by a Direct Packet support technician. ALL user configurable data WILL BE LOST! This process may render this system unusable! Click OK to continue or Cancel to abort.
OK
Cancel
Recover System
Main
Please Wait!
DO NOT INTERRUPT THIS PROCESS!!!
Restore started at: 16:09:37_05-18-2010
The restore should take no more than 10 minutes.
Rebooting. Watch the LCD for information.

The system can also be restored with the power button.

1) Power system on
2) Wait for "Remote Executive Office (REO)". This will only be displayed for four seconds.
3) Press power button three times.
4) Watch the LCD for details.

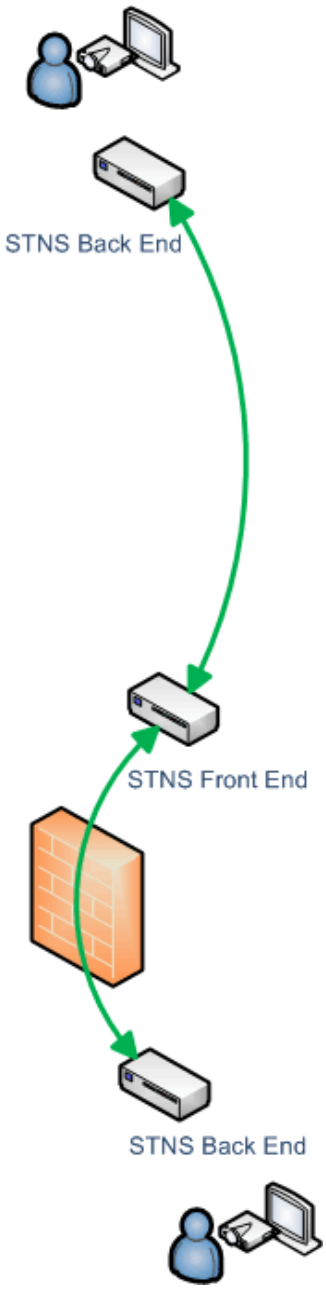
H.323 is a system specification and recommendation from the ITU Telecommunication Standardization Sector. H.323 is typically referred to as a protocol set for communication in audio and video across networks.

Because of H.323 complexities and various vendors, different ports are used for each call.

STNS is the Secure Traversal Navigation System which allows H.323 streaming over a single secure port.

## The STNS Stream

The STNS stream connects IPC-Routers to IPC-Controllers whether or not they are behind a firewall. The STNS stream does traverse firewalls, but it also secures those packets, wrapping them up in AES 256bit encryption (SSLv3/TLSv1) which is sent over the network using a single TCP port 443 by default.




### STNS:How it Works on Your Network

STNS is meant to perform several tasks while maintaining your current security policies and firewall configurations throughout your network. It is a gatekeeper, a firewall traversal system and a secure network appliance.

Placement: The Front End controller is meant to be placed out in the internet, beyond the firewalls and DMZ policies.

The IPC-Router is meant to reside somewhere inside the network, accessible by end points and other H.323 devices.

The IPC-Controller and IPC-Router talk through the firewall by wrapping the H.323 packets into one stream over port 443 using SSL version 3, encrypted using 256bit AES.

The IPC-Controller lives outside the firewall. It can be configured to work in the DMZ, however, if you plan on working within the DMZ, typical H.323 ports will need to be opened for proper H.323 communication to the internet.

# STNS:Logging In

Browse to the website specified in the setup. This will be http://thespecifiedIPaddress
Login with the following credentials:

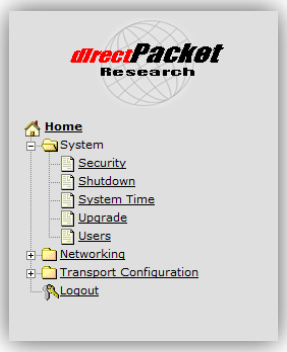
The default credentials are:

Username: admin
Password: 12pilot34

You can change these credentials at anytime under System – Users

The following screen will appear when you log in.

The following menu selections are located under the System menu



# System:Security:IP Access Control

This section allows you to limit which systems the STNS IPC-Controller or IPC-Router can administer. This can be performed by entering in IP Addresses, IP ranges, or domain names which will either be allowed or excluded from administering the unit. Configuring this section will prevent administering your Front End from an address outside of the network. If you choose to utilize the IP Access Control, give consideration to those who might need to troubleshoot the unit from a remote location.

Security
IP Access Control | SSL Encryption | Generate Request (CSR) | Upload New Certificate
The directPacket server can be configured to deny or allow access only from certain IP addresses using this form. Hostnames (like cracker.net) and IP networks (like 10.254.3.0 or 10.254.1.0/255.255.255.128) can also be entered. You should limit access to your server to trusted addresses, especially if it is accessible from the Internet. Otherwise, anyone who guesses your password will have complete control of your system.
IP Access Control
Access control options
Allow from all addresses
Only allow from listed addresses
Deny from listed addresses
Resolve hostnames on every request
Save

The directPacket graphical user interface can be configured to deny or allow access only from certain IP addresses or Hostnames. Examples: blackhat.net or 10.254.3.0 or 10.254.1.0/255.255.255.128. You should limit access to your server to trusted addresses, especially on a Front End Controller. Otherwise, anyone who guesses your password will have complete control of your system.

### Allow from all addresses (default)

Selecting this tab will allow access from any outside IP address. This would be considered low security.

### Only allow from listed addresses (recommended)

Selecting this tab will allow access from the IP addresses listed only, blocking attempts from anyone else.

### Deny from listed addresses

Selecting this tab will allow access from any outside IP address except those listed. This would be considered low security.

### Resolve hostnames on every request

Check this box if you want to increase security by running a reverse look-up.

## Configuration:Community Bridge

A Community Bridge is a means for joining two STNS communities together via an encrypted single port STNS stream.

**Requirements:**

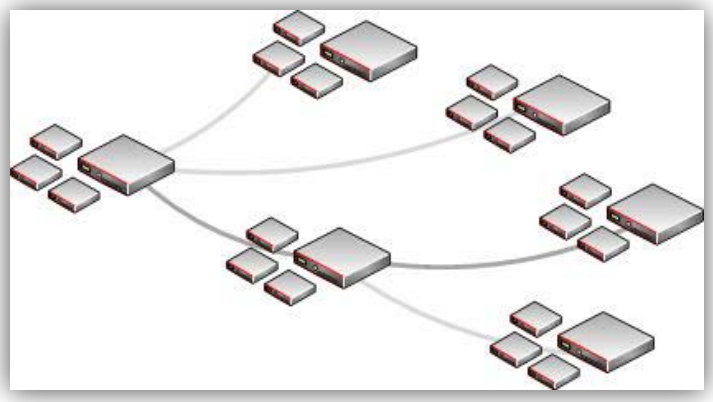
Default Community Key must be used
One Initiating Front End
One Target Front End
TCP Port 443 is used for communication

**Limitations:**

Each Front End has a maximum of three simultaneous connections. Those connections can either be inbound, outbound or a combination of both.

**Scaling Bridged Communities:**

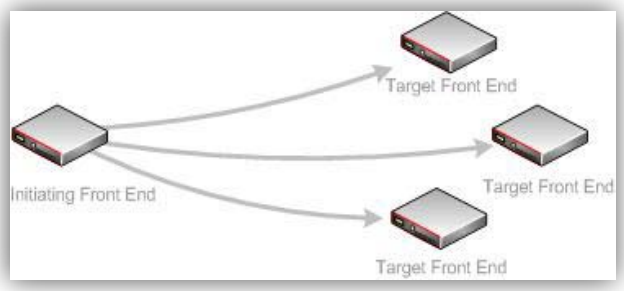
While each front end can be connected to three bridges, each connecting front end can be bridged into two more, and each of those into two more, and so on. This results in a highly scalable network.



**Creating a Community Bridge**

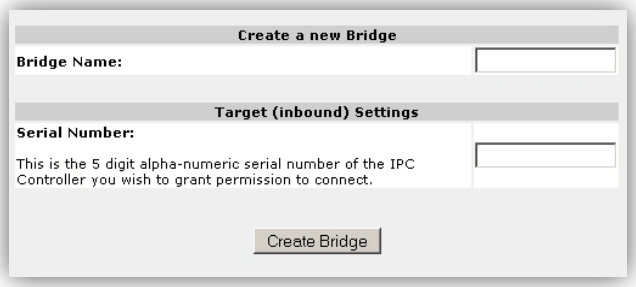
Each bridge connection must be configured from the source and the target. One front end controller is the source and the other front end controller is the target. Each setting must be configured on each side.

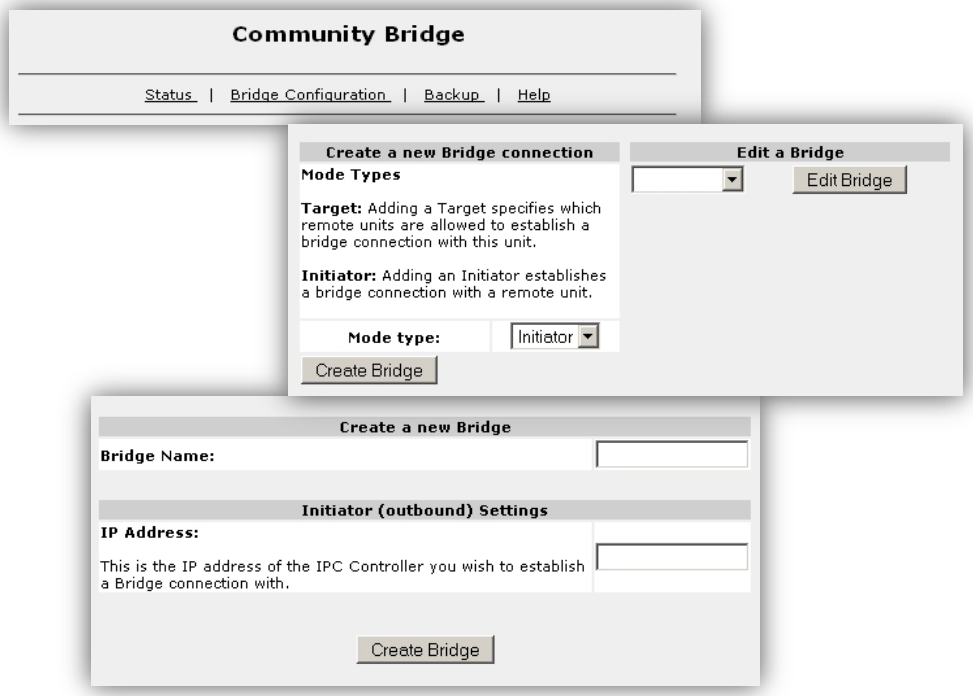
First, decide which will be the initiator and which will be the target.



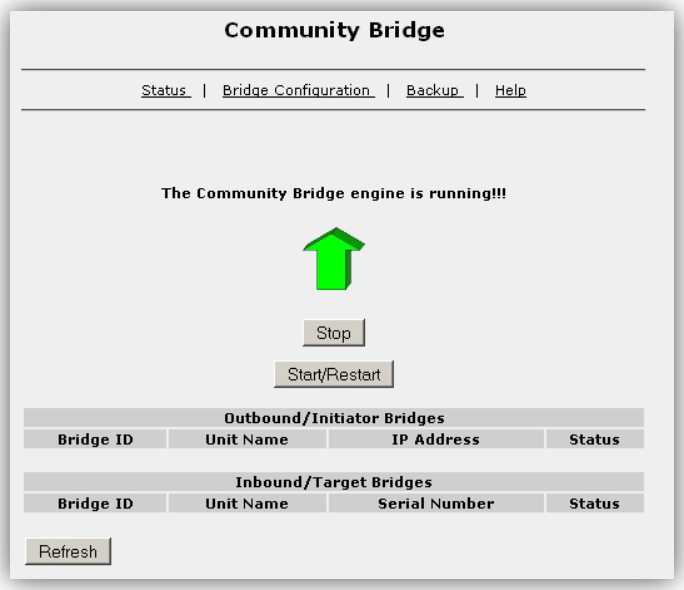

Start with the Target first. The Target must be configured with the Intiator's serial number. This is to allow permission to connect. Once complete, the initiating unit creates an "Initiator" bridge connection, which contains a name and the Target unit's publicly accessible IP address. Each bridge connection will be established over a single TCP stream which can easily pass through firewalls and routers without any additional configuration.

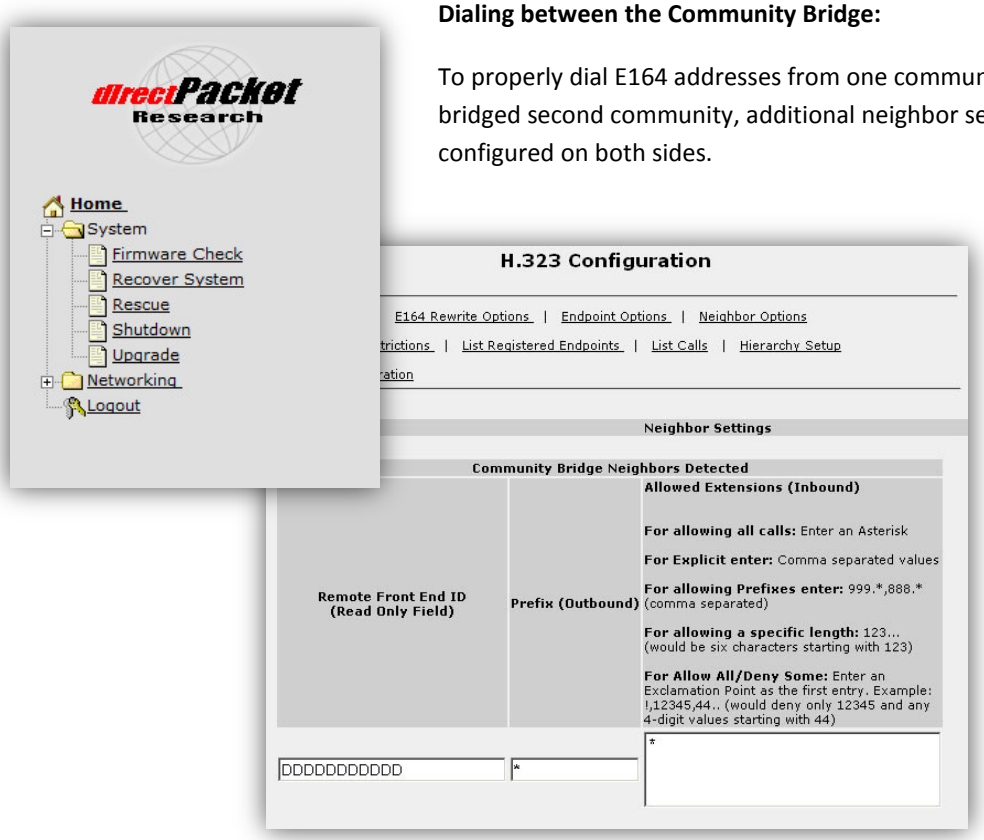
Community Bridge
Status | Bridge Configuration | Backup | Help
Create a new Bridge connection
Mode Types
Target: Adding a Target specifies which remote units are allowed to establish a bridge connection with this unit.
Initiator: Adding an Initiator establishes a bridge connection with a remote unit.
Mode type:
Target
Create Bridge
Edit a Bridge
Edit Bridge


Create a new Bridge
Bridge Name:
Target (inbound) Settings
Serial Number:
This is the 5 digit alpha-numeric serial number of the IPC Controller you wish to grant permission to connect.
Create Bridge


Community Bridge
Status | Bridge Configuration | Backup | Help
Create a new Bridge connection
Mode Types
Target: Adding a Target specifies which remote units are allowed to establish a bridge connection with this unit.
Initiator: Adding an Initiator establishes a bridge connection with a remote unit.
Mode type:
Initiator
Create Bridge
Edit a Bridge
Edit Bridge
Create a new Bridge
Bridge Name:
Initiator (outbound) Settings
IP Address:
This is the IP address of the IPC Controller you wish to establish a Bridge connection with.
Create Bridge

Once these steps are complete, you can start each of the services on each of the front end controllers. This will bridge the two communities together through an STNS stream.




directPacket Research
Home
System
Firmware Check
Recover System
Rescue
Shutdown
Upgrade
Networking
Logout
H.323 Configuration
E164 Rewrite Options | Endpoint Options | Neighbor Options
trictions | List Registered Endpoints | List Calls | Hierarchy Setup
ration
Neighbor Settings
Community Bridge Neighbors Detected
Remote Front End ID (Read Only Field)
Prefix (Outbound)
Allowed Extensions (Inbound)
For allowing all calls: Enter an Asterisk
For Explicit enter: Comma separated values
For allowing Prefixes enter: 999.*,888.* (comma separated)
For allowing a specific length: 123... (would be six characters starting with 123)
For Allow All/Deny Some: Enter an Exclamation Point as the first entry. Example: !,12345,44.. (would deny only 12345 and any 4-digit values starting with 44)
DDDDDDDDDDD
*
*

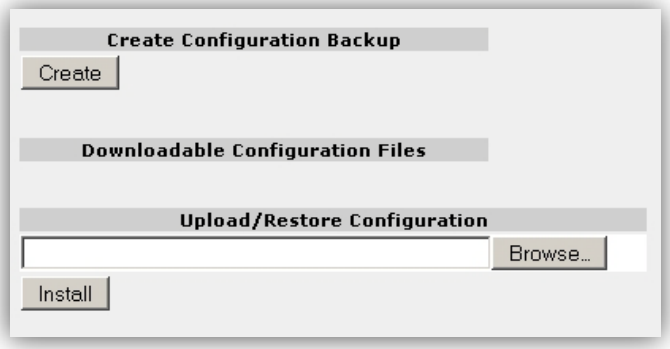
**Dialing between the Community Bridge:**

To properly dial E164 addresses from one community to a community bridged second community, additional neighbor settings will need to be configured on both sides.

H323: Permissions for routes can be made through Neighboring under the Transport Configuration | H323 Configuration.

SIP: Permissions for routes can be made through Trunking under the Transport Configuration | SIP Configuration

Backups in the community bridge section only backup this configuration.



# System:Security:SSL Encryption

The SSL Encryption section will allow administration of the STNS unit through SSL. Once it is set up, you will only be able to access the site via: https://controllerIPaddress, where the IP address or name resolves to the unit.

NOTE: You must refresh your browser window after enabling or disabling SSL.

### Enable SSL?

Use this to enable or disable SSL encryption for the graphical interface (GUI).

### Change Certificate File

Click **browse** and select the correct .pem file in the new window and click **OK**. Verify your selection in the text box, Click **SAVE** and refresh your browser.

Warning - SSL requests for this web server will use port 563 or 8443. STNS controllers use these ports because STNS uses 443 for firewall traversal. Only enable SSL here if your firewall and/or HTTP proxy server allows outbound SSL requests on port 563 or 8443, or else you will get locked out of the interface.

After enabling SSL, close your browser window and access this interface as demonstrated below:

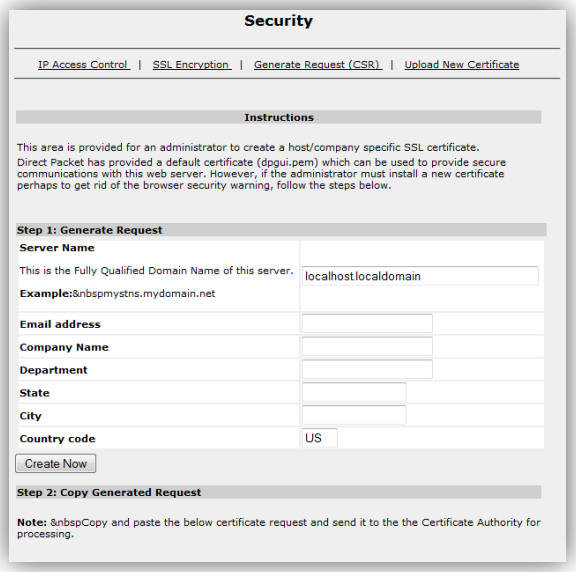
Security
IP Access Control | SSL Encryption | Generate Request (CSR) | Upload New Certificate
SSL Encryption
Warning - SSL requests for this web server can use port 80, 563 or 8443. This is because STNS uses 443. Only enable SSL here if your firewall and/or HTTP proxy server allows outbound SSL requests on the chosen port or else you will get locked out of this interface.
After enabling SSL, close your browser window and access this interface as demonstrated below:
https://your_ip_here:563
Enable SSL?
Yes
No
SSL TCP Port
80
Change Certificate File
/dpgui.pem
...
Save

When you are finished editing the fields on this page click **SAVE** to make changes take effect.

# System:Security:Generate Requesst (CSR)

The default Certificate will provide the same level of security as a signed certificate. The only difference is the client web browser will display a security warning when accessing the page.

The STNS Graphical User Interface (GUI) provides the ability of installing a signed certificate from a Certificate Authority. Certificate Authorities typically require the administrator to provide a Certificate Request or a CSR. This page has been made available to create a CSR.


Security
IP Access Control | SSL Encryption | Generate Request (CSR) | Upload New Certificate
Instructions
This area is provided for an administrator to create a host/company specific SSL certificate.
Direct Packet has provided a default certificate (dpgui.pem) which can be used to provide secure communications with this web server. However, if the administrator must install a new certificate perhaps to get rid of the browser security warning, follow the steps below.
Step 1: Generate Request
Server Name
This is the Fully Qualified Domain Name of this server.
Example:&nbspmystns.mydomain.net
localhost.localdomain
Email address
Company Name
Department
State
City
Country code
US
Create Now
Step 2: Copy Generated Request
Note: &nbspCopy and paste the below certificate request and send it to the the Certificate Authority for processing.

To create a CSR:

1. Disable SSL if it is currently on. To disable SSL, Navigate to System, Security, and then SSL Encryption. Change “Use SSL?” to No.
2. Navigate to System, Security, then Generate Request (CSR)
3. Fill out the request form with your company specifics.
4. Click “Create Now”.
5. A CSR will appear at the bottom of the page. Copy and paste this information into a text file and send it to the Certificate Authority for processing.
6. After the Certificate Authority sends a certificate back, navigate to System, Security, and then Upload New Certificate.
7. Click Browse to locate the certificate on your workstation hard disk.
8. Click Install.
9. Navigate back to System, Security, and then SSL Encryption.
10. Click the file chooser button in the Change Certificate File field and select the new certificate.
11. Change “Use SSL?” to Yes.
12. Click Save.

It is recommended to close you browser window and launch a new one. The administration GUI can be access now via port 563 or 8443, whichever you chose.

Example: https://<your_ip_here>:563
https://<your_ip_here>:8443

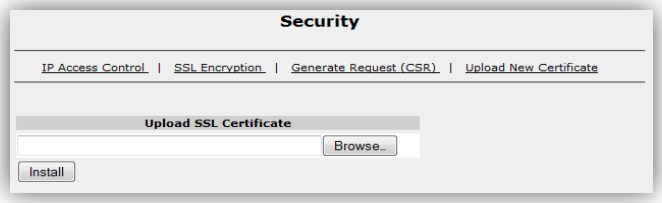
# System:Security:Upload New Certificate

Warning: Only files with the extensions of .PEM and .CER should be uploaded.

## Upload File

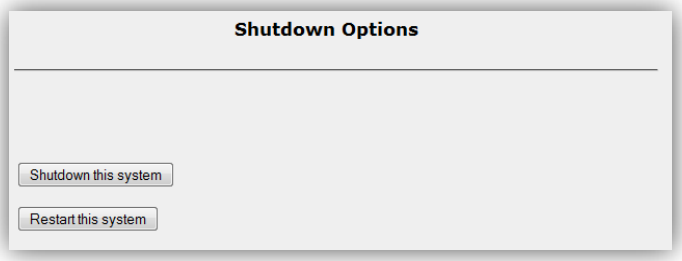
Click **Browse** and navigate to the location of your .PEM or .CER backup files. Double click on the file you wish to upload. Click **Install**.

To use this new certificate follow the instructions listed in the above section titled **Generate CSR**.


Security
IP Access Control | SSL Encryption | Generate Request (CSR) | Upload New Certificate
Upload SSL Certificate
Browse...
Install

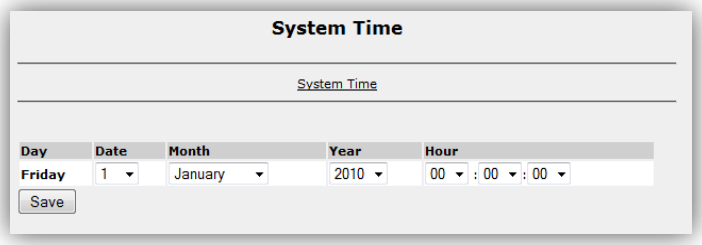
# System:Shutdown

This provides ability to shut down or restart the system. Shutting down the system requires a physical recycling of power on models FE, EBE, and REO. Both of the actions on this page will stop all STNS functionality. These actions should only be taken in an IT down time window.



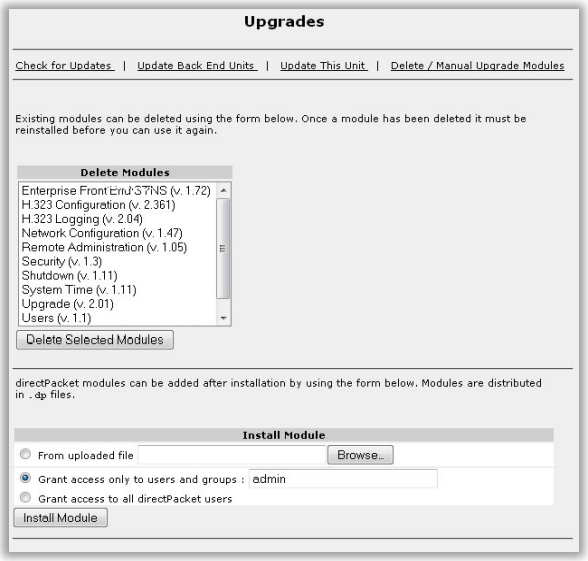

# System:System Time

The STNS systems do not allow any NTP servers to sync the time. Time is set in this section.



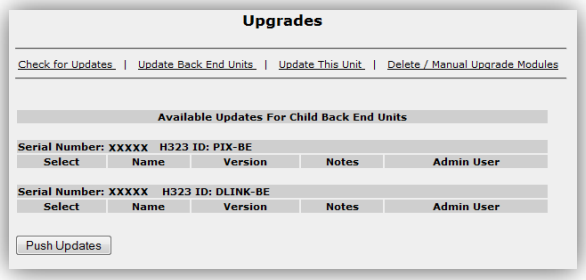
# System:Upgrade

Software updates are done under advisory from directPacket. These updates will not be available for your unit(s) until they are authorized and tested from directPacket. The updates will be performed by a directPacket technician over the phone to ensure the devices are in proper working order.


Upgrades
Check for Updates | Update Back End Units | Update This Unit | Delete / Manual Upgrade Modules
Existing modules can be deleted using the form below. Once a module has been deleted it must be reinstalled before you can use it again.
Delete Modules
Enterprise Front End STNS (v. 1.72)
H.323 Configuration (v. 2.361)
H.323 Logging (v. 2.04)
Network Configuration (v. 1.47)
Remote Administration (v. 1.05)
Security (v. 1.3)
Shutdown (v. 1.11)
System Time (v. 1.11)
Upgrade (v. 2.01)
Users (v. 1.1)
Delete Selected Modules
directPacket modules can be added after installation by using the form below. Modules are distributed in .dp files.
Install Module
From uploaded file
Browse...
Grant access only to users and groups : admin
Grant access to all directPacket users
Install Module

## Delete Modules

In this section the administrator can select modules to be deleted. In the text box, highlight the module to be deleted and click Delete Selected Modules. You will be redirected to a confirmation page. Review the modules due to be deleted, put a check in the check box and click delete.


Upgrades
Check for Updates | Update Back End Units | Update This Unit | Delete / Manual Upgrade Modules
Available Updates For Child Back End Units
Serial Number: XXXXX H323 ID: PIX-BE
Select Name Version Notes Admin User
Serial Number: XXXXX H323 ID: DLINK-BE
Select Name Version Notes Admin User
Push Updates

TIP! Multiple modules can be selected by holding CTRL and clicking on the modules.

CAUTION! Once a module has been deleted it must be reinstalled before you can use it again.

## Install Module

directPacket modules can be added after installation. Modules are distributed in .dp files.

## From Uploaded File

Click **Browse** and navigate to the location of your STNS module files. Double click on the module you wish to install.

## Grant access only to users and groups (default)

Click this tab and specify the users and groups you wish to grant access to this module. This can also be done in the section **Users** at a later time. Default user is admin.

## Grant access to all users

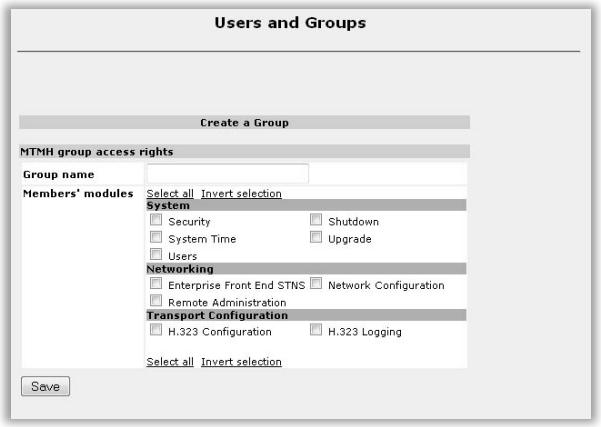
Alternately you can select this tab to allow anyone with valid login credentials access to the new module. When you are finished editing the fields in this section click **Install Module** and you will be redirected to a success page.

When upgrading, you will also be prompted for updates to any IPC-Router that is connected to the IPC-Controller you are updating. Each Child IPC-R will be listed with applicable updates.

# System:Users

This section allows the STNS administrator to create and edit the permissions of STNS groups and users.

## Create New User




Click **Create New User** to be redirected to the User Access Rights page. Select a name for the new user. In the drop down box select set to and in the next text box enter a password for the new user.

## Modules

Select the modules that the user will be given access or click **Select All** to allow this user full access. If you are editing an existing user who is the member of a certain group(s), the modules selected here are will be added to this user only.

When you are finished editing the fields in this section click **Save** and you will be redirected to the main user page and will see the new user listed.

Once a user exists, the administrator can edit all aspects of the user's credentials and permissions by simply clicking on the users name or their list of permitted modules. Additionally, if you have created groups you can add each user to a specific group.

## Create New Group

Click Create New Group to be redirected to the Create a Group page.

## Group Name

Select a name for this group of users. e.g. JrAdmins

## Member's Modules

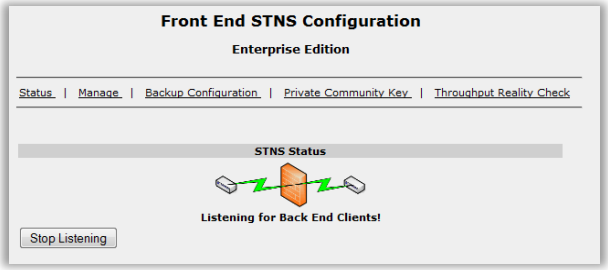
Select the modules that this group will be given access or click **Select All** to allow this group full access to all modules.

When you are finished editing the fields in this section click **Save** and you will be redirected to the main user page and will see the new group listed.

Once a group exists, the administrator can edit all aspects of the group's credentials and permissions by simply clicking on the group name or its list of permitted modules. Additionally, you can now add members to a group by clicking on the user and in the field "Member of Group" selecting the appropriate group name and clicking **Save**.

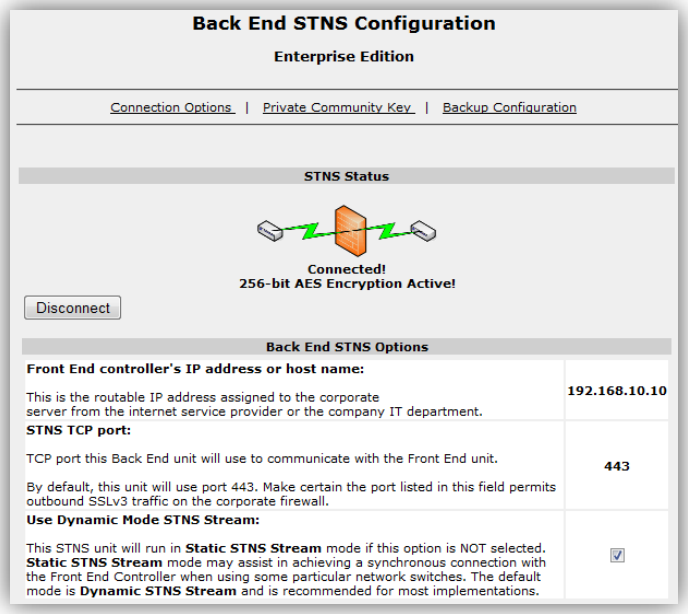
## Networking:Enterprise Front End STNS:Status

The Front End STNS will need to be turned on by clicking on Start Listening. Once this is performed, the IPC-Controller will be listening for IPC-R clients to connect through the STNS stream.


Front End STNS Configuration
Enterprise Edition
Status | Manage | Backup Configuration | Private Community Key | Throughput Reality Check
STNS Status
Listening for Back End Clients!
Stop Listening

## Networking:Enterprise Back End STNS:Status

By default STNS status is "Not Connected".


Back End STNS Configuration
Enterprise Edition
Connection Options | Private Community Key | Backup Configuration
STNS Status
Connected!
256-bit AES Encryption Active!
Disconnect
Back End STNS Options
Front End controller's IP address or host name:
This is the routable IP address assigned to the corporate server from the internet service provider or the company IT department.
192.168.10.10
STNS TCP port:
TCP port this Back End unit will use to communicate with the Front End unit.
By default, this unit will use port 443. Make certain the port listed in this field permits outbound SSLv3 traffic on the corporate firewall.
443
Use Dynamic Mode STNS Stream:
This STNS unit will run in Static STNS Stream mode if this option is NOT selected. Static STNS Stream mode may assist in achieving a synchronous connection with the Front End Controller when using some particular network switches. The default mode is Dynamic STNS Stream and is recommended for most implementations.

### IPC-Router STNS Options

IPC-C's IP address or host name. Enter the routable IP address assigned to the corporate IPC-C from the internet service provider or the company IT department. E.g. 26.218.X.X If this address is not valid the STNS process will fail!

### STNS TCP port

Enter the TCP port this IPC-Router unit will use to communicate with the Front End unit.

E.g. 443 (default). Make certain the port listed in this field, if other than 443, permits outbound SSLv3 traffic on the corporate firewall.

If there is no proxy server then you may leave the rest of the fields blank and that is all you need. If there is an HTTP Proxy server skip to section "Proxy Server Configuration."

If you are finished editing the fields in "Back End STNS Options," click "Connect" to begin the STNS process. If you are successful you will be redirected to the "STNS Status" page where you will see the "Connected!" symbol and "256-bit AES Encryption Active!" text. You can now move to section "Transport Configuration."

WARNING! If you for any reason you need to restart or power down the STNS unit click **Disconnect** onthis page before doing so.

### Proxy Server Configuration (Optional)

#### HTTP proxy IP or hostname

Enter the IP Address or hostname of the proxy server.
E.g. SQUID-SERVER
NOTE: This option is only applicable if the STNS TCP port listed above is 80 or 443.

#### TCP port your HTTP proxy uses

Enter the port number used by the proxy server.
E.g. 8080
NOTE: Mandatory if HTTP proxy is being used.

#### HTTP proxy user name

Enter the user name used to authenticate to the HTTP proxy server.

#### HTTP proxy password

Enter the password used to authenticate to the HTTP proxy server.

### Use Integrated Windows Authentication

Select this option if your proxy server is Microsoft Proxy or ISA server and uses Integrated Windows, NTLM or Active Directory authentication.

NOTE: Leave this field blank for Base64 encoding or Basic Authentication.

### Active Directory Domain Name

Enter the Active Directory domain here. E.g. ADDOMAIN

NOTE: This is only applicable if using IWA authentication.

### Active Directory Hostname

Enter the computer name you wish Active Directory to see this STNS unit as. E.g. STNSBE

NOTE: This option is useful when Active Directory domain resources are restricted to specific hosts.

**NOTE: This is only applicable if using IWA authentication.**

When you are finished editing the fields on this page click “Connect” to begin the STNS process. If you are successful you will be redirected to the “STNS Status” page where you will see the “Connected!” symbol and “256-bit AES Encryption Active!” text.

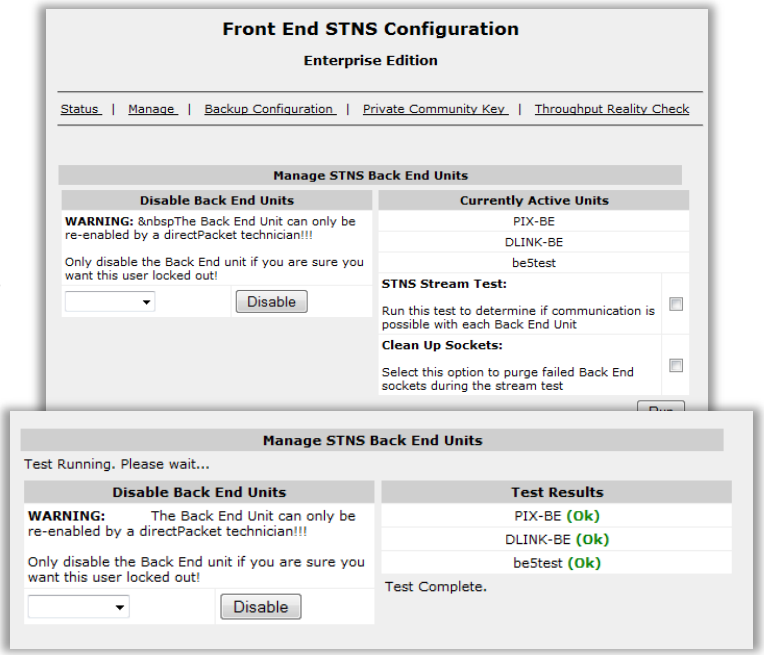
# Networking:Enterprise Front End STNS:Manage

This section allows you to test the front end and back end connectivity. The test will only make sure the STNS stream is up and running.

There is an option to clean up the ports, which will flush out current connections. This is not recommended for active sessions.

There is also the ability to disable an IPC-Router or REO unit. When this is performed, the disabled unit will no longer function, nor will it be able to connect to any IPC-Controller.

**Performing this action is not reversible.**


Front End STNS Configuration
Enterprise Edition
Status | Manage | Backup Configuration | Private Community Key | Throughput Reality Check
Manage STNS Back End Units
Disable Back End Units
WARNING: &nbspThe Back End Unit can only be re-enabled by a directPacket technician!!!
Only disable the Back End unit if you are sure you want this user locked out!
Disable
Currently Active Units
PIX-BE
DLINK-BE
be5test
STNS Stream Test:
Run this test to determine if communication is possible with each Back End Unit
Clean Up Sockets:
Select this option to purge failed Back End sockets during the stream test
Manage STNS Back End Units
Test Running. Please wait...
Disable Back End Units
WARNING: The Back End Unit can only be re-enabled by a directPacket technician!!!
Only disable the Back End unit if you are sure you want this user locked out!
Disable
Test Results
PIX-BE (Ok)
DLINK-BE (Ok)
be5test (Ok)
Test Complete.

# Networking:Enterprise Front End STNS:Backup Configuration

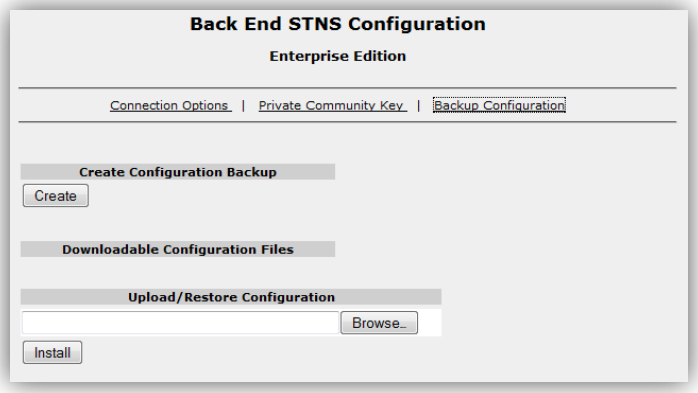
Your current configuration can be backed up.

## Create Backup Configuration

Click **Create** to generate a backup of the current configuration.

## Downloadable Configuration Files

Click on the underlined .dp file you wish to save to your workstation. WITHOUT CHANGING THE NAME OR FILE EXTENSION, select a location and folder to store your STNS backup files. Click **Save**. Click **Close**.

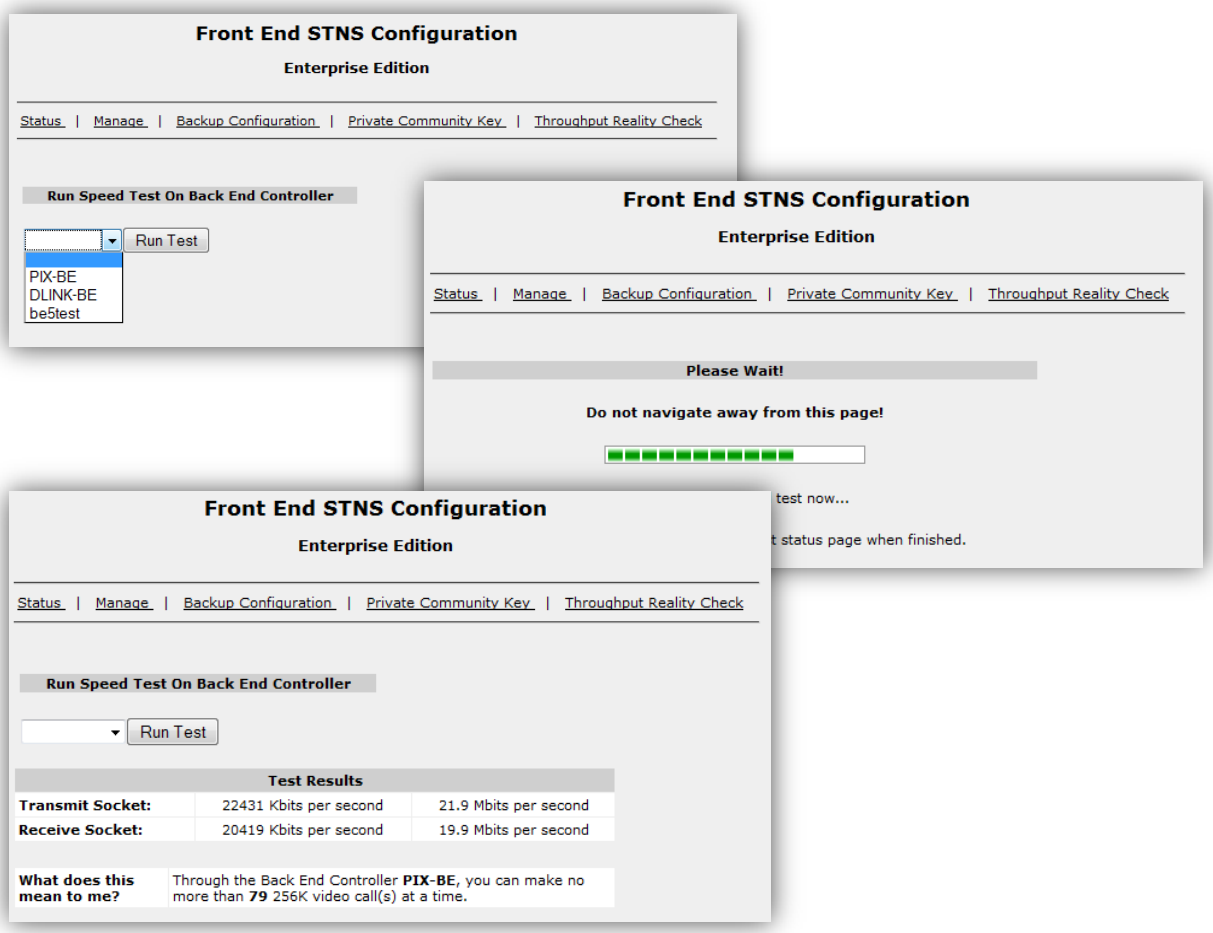



## Upload/Restore Configuration

Click **Browse** and navigate to the location of your STNS backup files. Double click on the backup you wish to restore. Click **Install** You will receive a "Configuration Installed!" message.

## Networking:Enterprise Front End STNS:Throughput Reality Check

Provides ability to do a speed check to a specified Back End Controller. This action only tests the STNS stream between the Front End and Back End controllers.


Front End STNS Configuration
Enterprise Edition
Status | Manage | Backup Configuration | Private Community Key | Throughput Reality Check
Run Speed Test On Back End Controller
Run Test
PIX-BE
DLINK-BE
be5test
Front End STNS Configuration
Enterprise Edition
Status | Manage | Backup Configuration | Private Community Key | Throughput Reality Check
Please Wait!
Do not navigate away from this page!
test now...
t status page when finished.
Front End STNS Configuration
Enterprise Edition
Status | Manage | Backup Configuration | Private Community Key | Throughput Reality Check
Run Speed Test On Back End Controller
Run Test
Test Results
Transmit Socket: 22431 Kbits per second 21.9 Mbits per second
Receive Socket: 20419 Kbits per second 19.9 Mbits per second
What does this mean to me? Through the Back End Controller PIX-BE, you can make no more than 79 256K video call(s) at a time.

## Networking:Network Configuration:Interface Options

In the field titled **Active Network Interfaces** click on **eth0** to be redirected to the "Boot Time Interface Parameters" page for the selected interface.

Static field will always be named "Eth0".

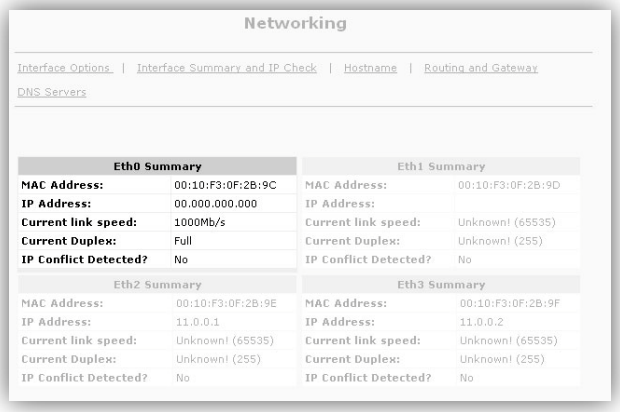
### From DHCP (default)

Select this radio button if you wish to have the network setting automatically assigned by a DHCP server.

NOTE: With DHCP selected you do not need to complete the rest of this form and you are finished with this section.

### From BOOTP

Select this radio button if you wish to have the network setting automatically assigned by a BOOTP server.




### Static (recommended)

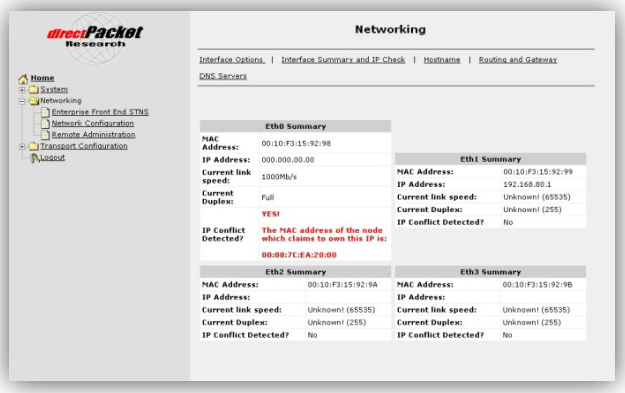
Select the last tab and enter the static IP Address you wish to give this STNS unit. e.g. 192.168.X.X This address should be outside of all DHCP scopes.

### Netmask

Enter the Subnet Mask for this STNS unit. e.g. 255.255.255.0

### Broadcast

Enter the broadcast address for this STNS unit. e.g. 192.168.X.255




### MTU

Enter the MTU for this STNS unit. e.g. 1500

When you are finished editing the fields on this page click **SAVE** to be redirected to the main networking page. Click **Save and Apply** if you wish to apply the changes immediately and refresh the interface.

At the bottom of this page you will notice a field entitled Eth0 Summary. This allows you to see the fundamental settings for this adapter.

NOTE: We strongly recommend that your link speed and duplex be at least 100Mb/s FULL.

## Networking:Network Configuration:Interface Summary and IP Check

When you pull up the Interface Summary and IP Check, the interfaces will be polled at that moment. They are not cached in the system. Verify the link speed and if any IP conflicts are present.

If there is an IP conflict, it needs to be resolved prior to any further troubleshooting.

## Networking:Network Configuration:Hostname

Enter the Hostname and Domain Name of this system. A Reboot is required in order the name change to take effect.

## Networking:Network Configuration:Routing and Gateway

### Default Gateway

From the dropdown box, select “eth0” and in the textbox labeled “Gateway”. Enter the IP Address of the default gateway for this STNS unit. E.g. 10.0.0.1

### Static Routes

Static routes may be specified for advanced STNS implementations.

### Active Routes

This is a display of the current routing table.

When you are finished editing the fields on this page click **SAVE**. Navigate back to the main networking page. Click **Apply Configuration** for the changes to take effect.

NOTE: This action will cause the network adapters to refresh. You will notice a pause and then be reconnected.

Warning! This may make your system inaccessible via the network, and cut off access to this machine if improperly configured.

## Networking:Network Configuration:DNS Servers

Enter the IP address(s) of the DNS servers you wish to use.
NOTE: This field is not required and may be left blank.

When you are finished editing the fields on this page click **SAVE** to be redirected to the main networking page.

## Networking:Remote Administration

This allows you to control the Back End configuration from the Front End. Authentication to the selected Back End must be supplied.

Remote Administration
Home
Connect to Back End Graphical Interface
This tool is only intended to allow administrators to modify or adjust the Transport Configuration options of, or apply updates to STNS Back End units from this STNS Front End controller. The interface appears as if the administrator were connecting to the graphical interface of the Back End unit.
Modifying the STNS stream in such a way as disconnecting or reconnecting, changing Private Community Keys or changing network settings is not supported using this tool.
File uploads to Back End units are not available through this portal.
Click on the provided link below. A new browser window will be opened. If you have a Pop-up blocker, you may need to configure it to allow this action. If you cannot configure your Pop-up blocker to allow this action, copy and paste the below link into a new browser window or browser tab.
Multiple Back End units may be administered by opening the below link in multiple windows or tabs.
http://22.222.222.222/remoteCtrl/stns-manage.cgi

## TransportConfiguration:H.323 Configuration:E164 Rewrite Options

**Original E164 or Incoming Prefix**

The original E164 as received from endpoint or gateway. E.g. 1234

**Rewrite to (Enter a Space to strip)**

The E164 as you wish it to be rewritten and identified by this unit. E.g. 4321

This feature is extremely useful in larger networks and communities that are either neighbored or registered with each other, and have duplicate E164 numbers. Say that locations “A” and “B” both have an E164 of 1234 registered to it, to allow them to call the correct far endpoint Company “A” would set Source “4321” = Destination “1234” and company “B” would set Source “321” = Destination “1234”. So when “A” dials “321” “B” receives it and rewrites it to “1234”.

When you are finished editing the fields on this page click “SAVE” and then click “Apply Configuration” for the changes to take effect. Click **Save Changes Only** if you do not wish to apply the changes immediately.

NOTE: This is a runtime operation it will not drop all calls. To delete an entry simply highlight and erase.

## TransportConfiguration:H.323 Configuration:Endpoint Options

**Endpoint IP Address**

The IP address of the static endpoint or gateway an administrator wishes to set for a permanent registration.
E.g. 192.168.X.X

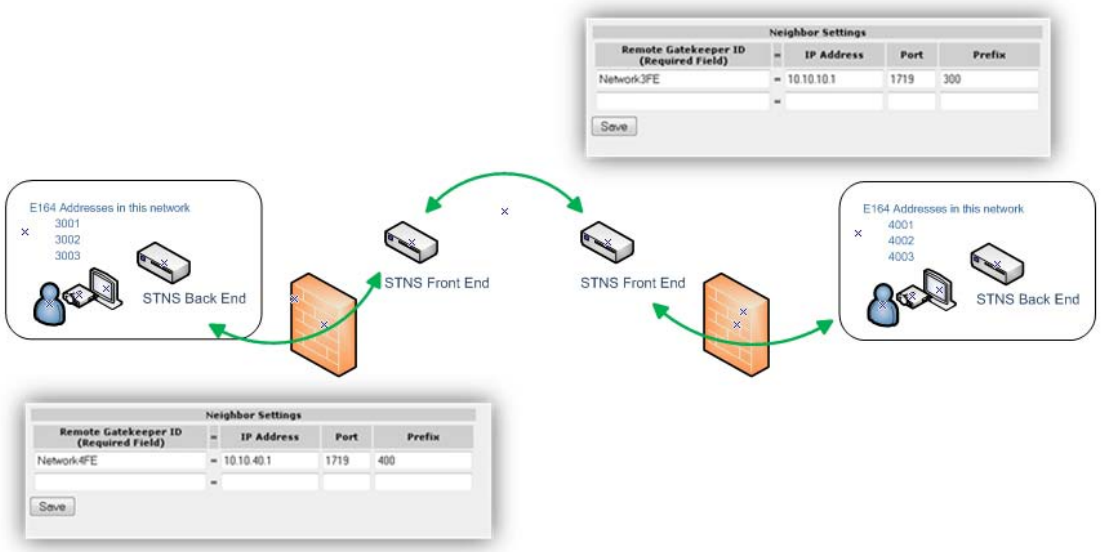
**E164; Prefix**

The E164 and prefix of the static endpoint or gateway an administrator wishes to set for a permanent registration. If the unit is an endpoint the prefix would be its E164.
E.g. Gateway MYGATEWAY;0010

# TransportConfiguration:H.323 Configuration:Neighbor Options

**Defining Neighbors**

Neighbors are setup for ease of calling between different Front Ends or sites. Neighbors are merely pointers on one device, which is not pushed to another device.




Given the above diagram, the network on the right will require the 300 prefix to reach 3001, 3002, and 3003 extensions. The network on the left will require the configuration below in order to reach the 4001, 4002, and 4003 extensions.

**Remote Gatekeeper ID** The H323ID of the gatekeeper you wish to neighbor with.

**Remote Gatekeeper IP address** The IP address of the gatekeeper you wish to neighbor with.

**Port** The TCP port used for RAS communication with the remote gatekeeper

**Prefix** The string of digits used to define whether or not to forward a call to the remote gatekeeper.

If you are neighboring 2 or more STNS Front End devices the neighboring section must be set on all devices individually. Most third party gatekeepers require additional setup.

When you are finished editing the fields on this page click **SAVE** and then click **Apply Configuration** for the changes to take effect. Click **Save Changes Only** if you do not wish to apply the changes immediately.

NOTE: This is a runtime operation it will not drop all calls. To delete an entry simply highlight and erase.

## TransportConfiguration:H.323 Configuration:Registration Restrictions

**Allow all outside endpoints and bridges to register**

Check this box if you wish to disable registration restrictions. Selecting this option will allow any outside H.323 user to register to your unit if they have your IP address. This is very useful if the second party is unwilling or unable to provide the necessary information. Use caution when selecting this option.

**H.323 ID**

The H323ID of the device you wish to allow access to your STNS community. This field is strongly recommended for organizational purposes. E.g. BOB-AT-HOME

**IP Address (Mandatory)**

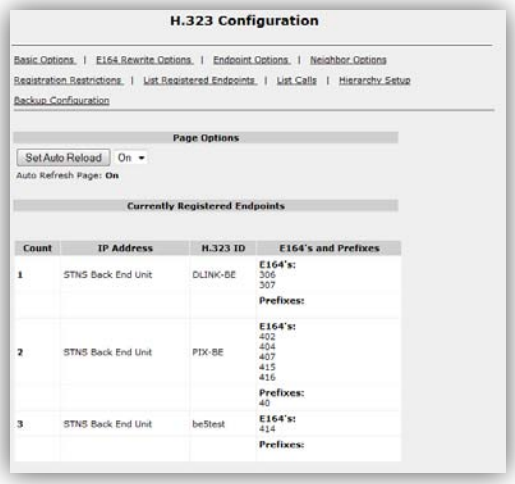
The IP address of the device you wish to allow access to your STNS community.
E.g. 22.175.X.X

When you are finished editing the fields on this page click “SAVE” and then click “Apply Configuration” for the changes to take effect.

Click “Save Changes Only” if you do not wish to apply the changes immediately.
NOTE: This is a runtime operation it will not drop calls unless you forget to add an address. To delete an entry simply highlight and erase.

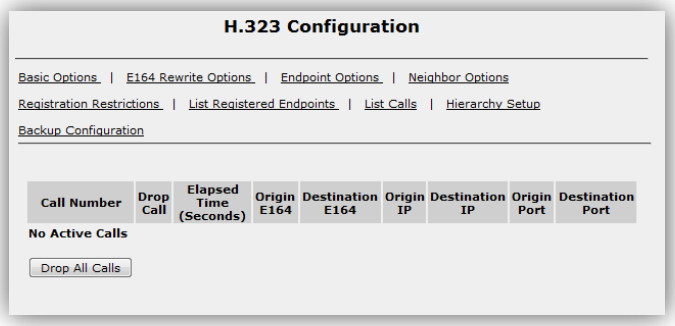
## TransportConfiguration:H.323 Configuration:List Registered Endpoint

This section is provided to allow the administrator or privileged user to view the endpoints, gateways, or bridges that are currently registered to STNS. Click “List Registered Endpoints” to refresh the list.



## TransportConfiguration:H.323 Configuration:List Calls

This section is provided to allow the administrator or privileged user to view the in-call status of endpoints, gateways, or bridges that are currently registered to STNS. Click “List Calls” to update the information.




## TransportConfiguration:H.323 Configuration:Hierarchy Setup

Hierarchy setup is necessary to notify the IPC-Controller of endpoints connected to the IPC-Router. The IPC-C does not fetch this information.

### Parent Gatekeeper

If a STNS stream has been established the STNS radio button will automatically be selected and the bottom banner will say “Front-End Controller Detected!” Select “none” to disable Hierarchy and disallow traversal calls. (Not recommended).

### E164 Digits

Manually set the E164 numbers of all endpoints granted permission to place and receive traversal calls in the textbox provided. Multiple E164’s must be comma separated. Or, follow the following steps for auto configuration. E.g. 1234,4567,7898,XXXX

### Auto Configure for STNS (Required)

Verify that all endpoints have successfully registered to the Back-End unit by checking the “List Registered Endpoints” section. Afterwards, navigate to the **Hierarchy Setup** page and place a check in the box and click **Auto Configure**. You will then see the E164 numbers of all endpoints granted permission to place and receive traversal calls in the “E164 Digits” textbox. Delete any duplicates and proceed.

When you are finished editing the fields on this page click **SAVE** and then click **Restart Gatekeeper** for the changes to take effect. Click “Save Changes Only” if you do not wish to apply the changes immediately.

NOTE: It is strongly recommended that you perform a **Restart Gatekeeper** only during IT downtime windows. All calls will be dropped when this action is taken.

# TransportConfiguration:H.323 Configuration:Backup Configuration

### Create Backup Configuration

Click **Create** to generate a backup of the current H.323 configuration.

### Downloadable Configuration Files

Click on the underlined .dp file you wish to save to your workstation. When prompted Click **Save** to continue or **Cancel** to stop saving. WITHOUT CHANGING THE NAME OR FILE EXTENSION, select a location and folder to store your STNS backup files. Click **Save**. Click **Close**.

### Upload/Restore Configuration

Click **Browse** and navigate to the location of your STNS backup files. Double click on the backup you wish to restore. Click **Install** You will receive a "Configuration Installed!" message. Navigate to the **Basic Options** section, click **Save** and click **Restart Gatekeeper**.

Click **Save Changes Only** if you do not wish to apply the changes immediately.

### Name of STNS Gatekeeper

The name (H323ID) by which this unit is identified. User defined.
E.g. FEGK1

### Bandwidth Management

This is the total allowed bandwidth (in Kilobits per second) through this controller.

When you are finished editing the fields on this page click "SAVE" and then click "Restart Gatekeeper" for the changes to take effect. Click **Save Changes Only** if you do not wish to apply the changes immediately.

*NOTE: It is strongly recommended that you perform a "Restart Gatekeeper" only during IT downtime windows. All calls will be dropped when this action is taken.*

# TransportConfiguration:H.323 Logging:Search the H323 Call & Debug Logging

**Log Size**
This field displays the current size of the log file. The call log will be deleted once it has reached 100MB in size.

**Search the H.323 Call Log**

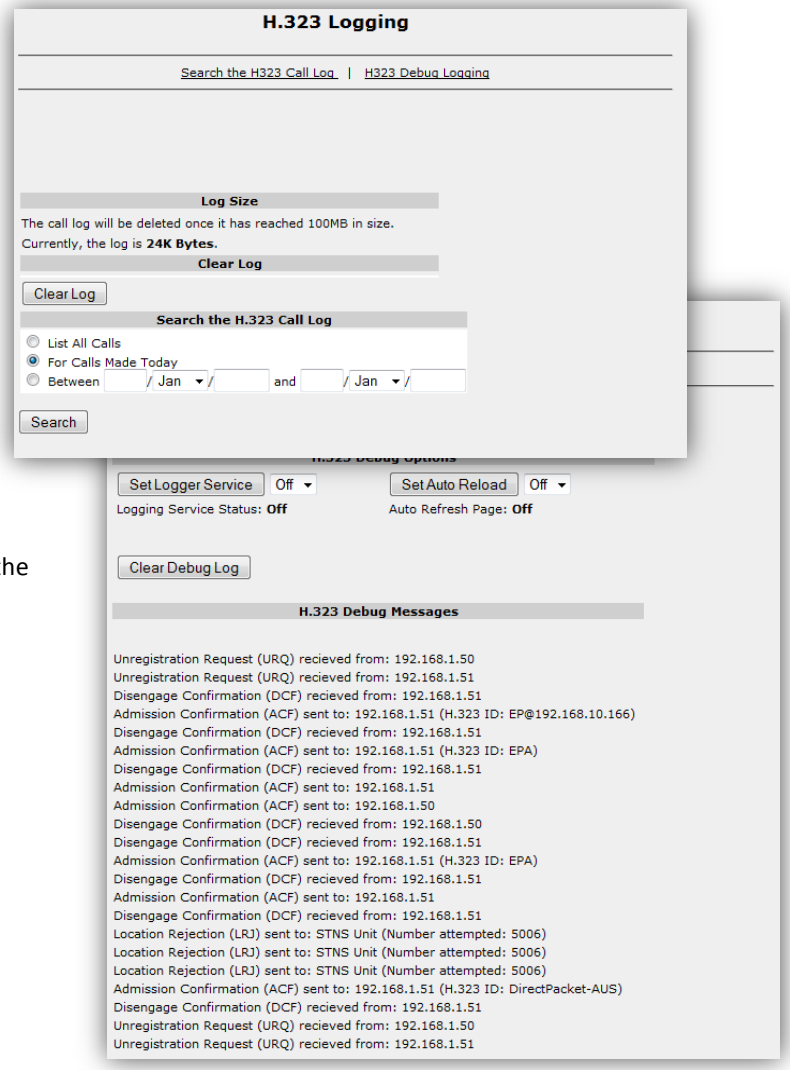
**List All Calls** When this option is selected all logged calls will be displayed. Click “Search”.

**For Calls Made Today** When this option is selected, only logged calls for today will be displayed. Click “Search”.

**Date range** Select a range of dates for logged calls. Click “Search”.

Follow the directions on the screen for saving the log files. To return to the selection page, click the “Search the H323 Log” tab at the top of the page.

Debug logging will show the call details for further troubleshooting.


H.323 Logging
Search the H323 Call Log | H323 Debug Logging
Log Size
The call log will be deleted once it has reached 100MB in size.
Currently, the log is 24K Bytes.
Clear Log
Clear Log
Search the H.323 Call Log
List All Calls
For Calls Made Today
Between / Jan / and / Jan /
Search
Set Logger Service Off
Logging Service Status: Off
Set Auto Reload Off
Auto Refresh Page: Off
Clear Debug Log
H.323 Debug Messages
Unregistration Request (URQ) recieved from: 192.168.1.50
Unregistration Request (URQ) recieved from: 192.168.1.51
Disengage Confirmation (DCF) recieved from: 192.168.1.51
Admission Confirmation (ACF) sent to: 192.168.1.51 (H.323 ID: EP@192.168.10.166)
Disengage Confirmation (DCF) recieved from: 192.168.1.51
Admission Confirmation (ACF) sent to: 192.168.1.51 (H.323 ID: EPA)
Disengage Confirmation (DCF) recieved from: 192.168.1.51
Admission Confirmation (ACF) sent to: 192.168.1.51
Admission Confirmation (ACF) sent to: 192.168.1.50
Disengage Confirmation (DCF) recieved from: 192.168.1.50
Disengage Confirmation (DCF) recieved from: 192.168.1.51
Admission Confirmation (ACF) sent to: 192.168.1.51 (H.323 ID: EPA)
Disengage Confirmation (DCF) recieved from: 192.168.1.51
Admission Confirmation (ACF) sent to: 192.168.1.51
Disengage Confirmation (DCF) recieved from: 192.168.1.51
Location Rejection (LRJ) sent to: STNS Unit (Number attempted: 5006)
Location Rejection (LRJ) sent to: STNS Unit (Number attempted: 5006)
Location Rejection (LRJ) sent to: STNS Unit (Number attempted: 5006)
Admission Confirmation (ACF) sent to: 192.168.1.51 (H.323 ID: DirectPacket-AUS)
Disengage Confirmation (DCF) recieved from: 192.168.1.51
Unregistration Request (URQ) recieved from: 192.168.1.50
Unregistration Request (URQ) recieved from: 192.168.1.51

# TransportConfiguration:Video Auto Attendant:Permissions

Extensions Allowed: Enter the E.164 numbers which are allowed to receive unregistered inbound calls. External calls destined for internal which are not listed here will be rejected by the Front End controller.

## TransportConfiguration:Video Auto Attendant:Static Forwarding

This feature is only used when the Video Auto Attendant is in Bridged mode.

Use this Static Forward Channel to allow a call from an endpoint or MCU which does not support DTMF dialing or cannot register to this Front End Controller.

Source IP: The IP address of the endpoint or MCU which will be calling in.
Destination Extension: The extension to which you wish the incoming call to be forwarded.
Activate check box: Determines whether or not this forwarder is active.

## TransportConfiguration:Video Auto Attendant:IP Restrictions

Security Check Log: This log contains the IP addresses which have failed the IP security check while attempting to make a call.

Blocked IP Addresses: Enter the IP address you wish to be blocked from making an H.323 call to this system. CIDR notation may be used to specify a network of hosts.

## TransportConfiguration:URI Dialing & SRV Record Requirements

When in Routed Mode, the Video Auto Attendant will accept calls in the format: e164@yourdomain.net. This function requires a SRV record to be created in your DNS forward lookup. SRV records are not required if the IP address or FQDN of the Front End controller is used instead of just the domain name.

The SRV record(s) should look similar to the following:

For H.323 Call Setup signaling:

_h323cs._tcp IN SRV 0 0 1720 fehostname.yourdomain.net.

For Location Requests and Location Confirmation (LRQ, LCF):

_h323ls._udp IN SRV 0 0 1719 fehostname.yourdomain.net.

Of course, there must be an A record for the host “fehostname.yourdomain.net” which points to the Front End controller in order for the above SRV record to resolve properly.

To check if a SRV record is configured properly using NSLOOKUP:

nslookup <press enter>
set type=SRV <press enter>
_h323cs._tcp.yourdomain.net <press enter>
_h323ls._udp.yourdomain.net <press enter>

The response should show the SRV request resolves to the Front End controller. If you receive a message stating anything other than this or “No Service location records”, then your DNS server is not properly configured.

# H.323:Video Auto Attendant

## Bridged mode

- Limited to three calls
- Splash Screen Auto Attendant
- Static Forwarding

Useful for using a splash screen auto-attendant.
The user can enter a particular E164 address.

Can utilize static forwarding – this is useful for ONE and only one IP address that is unable to dial via URI, DTMF nor is able to register to the FrontEnd. This allows that particular IP to forward directly to an endpoint once they try to initiate a call with the FrontEnd's IP.

In Bridged Mode permitted calls will be managed by the Front End controller. Outside callers will be greeted by an automated attendant and prompted to enter an e164 (extension) via DTMF (keypad on the callers remote). Call bandwidth will be limited to 384k and the video codec will be H.263. Bridged mode only answers calls that arrive from the Gb0/Eth0 network interface.

## Routed Mode

In Routed Mode permitted calls are passed through the STNS community without limiting the call bandwidth or codecs (H.263, H.264, ect...).

The endpoints participating in the call will negotiate directly with each other.

Outside callers place a call to an endpoint within the STNS community by dialing in URI format or: extension@IP (IP of Front End) or extension@hostname (hostname of Front End).

A default e164 address may be specified for callers who dial just the IP address of the Front End controller.

# Security:Private Community Keys

The STNS system allows for additional security by providing specialized keys for governing which Back End controllers are permitted to connect to a particular Front End controller. This enhanced level security is achieved by creating a Private Community Key on a Front End controller and then installing the Private Community Key on the Back End controller.

Follow to below steps to implement Private Community Keys on your STNS controllers.

1. Navigate to Networking | Enterprise Front End Controller | Private Community Key.
2. Click "Create" under "Create a new Community Key".

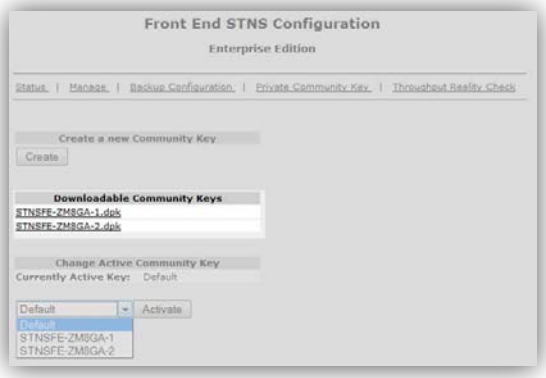
   The new key will show up under "Downloadable Community Keys" and also in the "Change Active Community Key" drop down box. The downloadable key will have the Front End Controller's serial number and the extension of DPK for easy identification.

3. Click on the key listed under "Downloadable Community Keys" to download to your workstation hard disk.
4. To enable a new Private Community Key on the Front End Controller, select a key from the drop down box under "Change Active Community Key" and click "Activate". The currently active key will be listed in the "Currently Active Key" area.

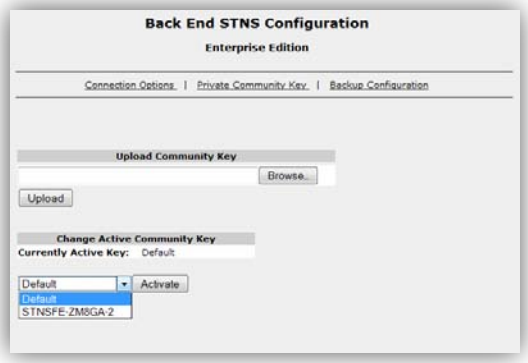
   Once a key has been activated on a Front End Controller, only Back End Controllers with the new key installed will be permitted to connect to the Front End Controller.

   A Default key is provided on all STNS Front and Back End units to allow for an open community. This default key cannot be removed.

   IMPORTANT: It is strongly recommended a "Backup Configuration" is performed immediately after activating a new Private Community Key. Private Community Keys are made to be unique and cannot be recreated in the event of a system disaster.



## Configuring each of the Back End Controllers



1. Navigate to Networking | Enterprise Back End Controller | Private Community Key
2. Click the “Browse” button to select the Private Community Key which is location on your workstation hard disk.
3. Click “Upload”. This installs the Private Community Key on the Back End controller, but does not activate it.
4. To activate an installed Private Community Key, select the key from the “Change Active Community Key” drop down box then click “Activate.”

## Troubleshooting:STNS Stream

The STNS stream is only going to flow between the Front End and Back End controllers. The stream can be up regardless of endpoint connectivity. The STNS stream is TLSv1 in addition to SSL version 3, which traverses the firewall on port 443.

Double check the IP and gateway settings in the networking - ETH0 configuration.

## Troubleshooting:EndPoint Issues

To properly troubleshoot endpoints, you will need to refer to the manual for specific endpoints.

Common issues we see with endpoints

Not able to register to the gatekeeper

- Verify the IP address settings are correct
- Verify that the subnet you are on will allow H.323 traffic.

Dialing and answering issues

- When dialing one endpoint inside

If the endpoint does not answer, check the auto attendant mode in the Transport Configuration

# Troubleshooting:Rescue Mode

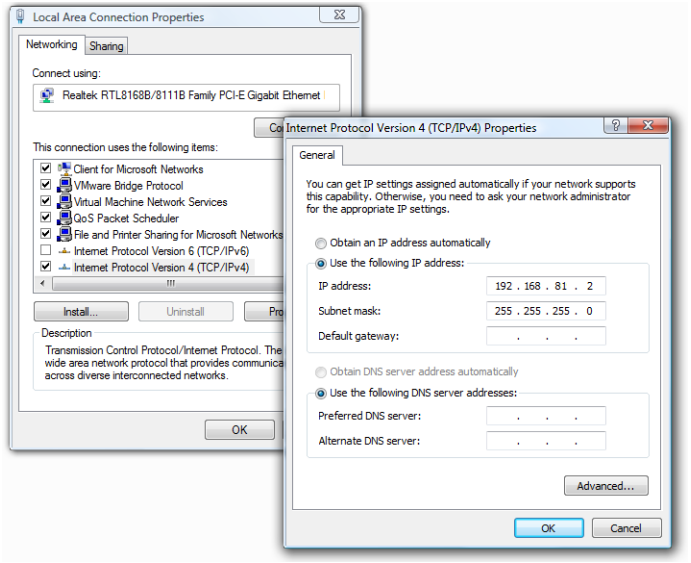
STNS controllers have a graphical interface which can perform rescue operations in the event of an emergency. Below is the list of tasks which can be performed while in Rescue Mode:

- Reset the admin password to 123456
- Reset all user accounts to factory defaults.
- Disable SSL mode on the master web user interface.
- Adjust network interface IP settings
- Restart or Shutdown the unit.

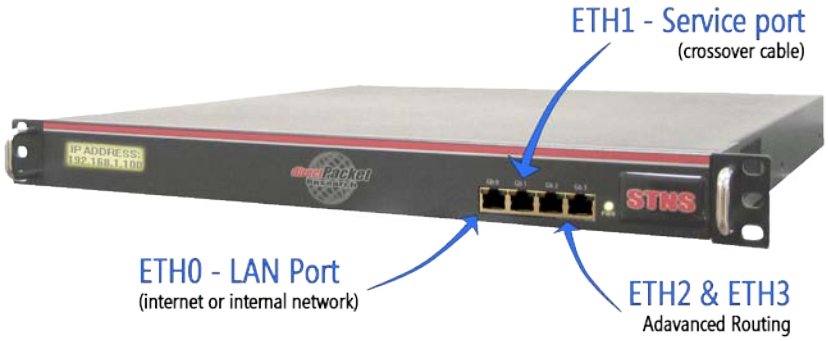
This special interface can only be accessed by connecting to the service port network interface (GB1) at the IP address of 192.168.81.1 with a tcp port of 911.

## Rescue Mode Setup

Just like the initial configuration of each controller, configure your notebook IP address to 192.168.81.2 with a subnet of 255.255.255.0.


Local Area Connection Properties
Networking
Sharing
Connect using:
Realtek RTL8168B/8111B Family PCI-E Gigabit Ethernet
This connection uses the following items:
Client for Microsoft Networks
VMware Bridge Protocol
Virtual Machine Network Services
QoS Packet Scheduler
File and Printer Sharing for Microsoft Networks
Internet Protocol Version 6 (TCP/IPv6)
Internet Protocol Version 4 (TCP/IPv4)
Install...
Uninstall
Description
OK
Internet Protocol Version 4 (TCP/IPv4) Properties
General
You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.
Obtain an IP address automatically
Use the following IP address:
IP address:
192 . 168 . 81 . 2
Subnet mask:
255 . 255 . 255 . 0
Default gateway:
Obtain DNS server address automatically
Use the following DNS server addresses:
Preferred DNS server:
Alternate DNS server:
Advanced...
OK
Cancel

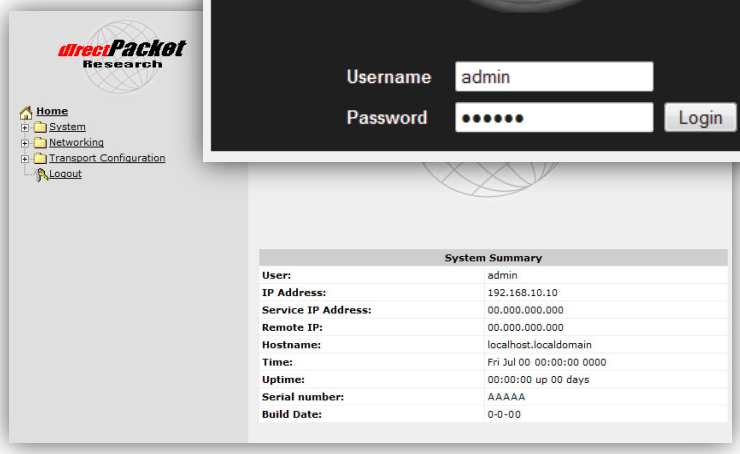
Connect a notebook via the service port on the STNS unit using a crossover cable.



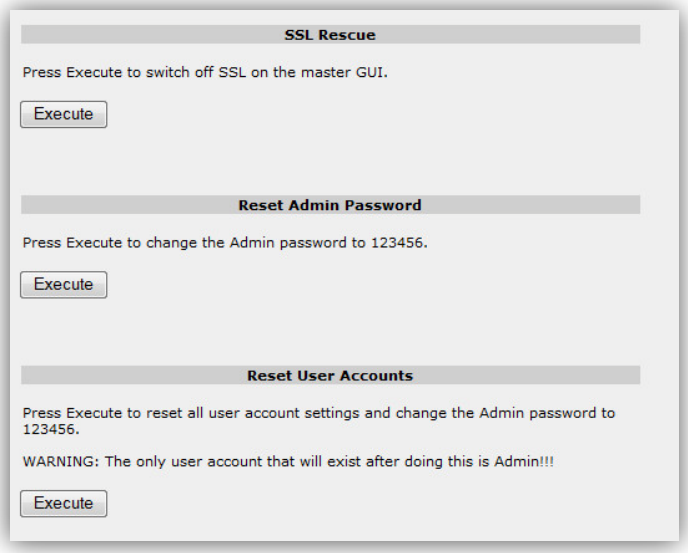

Open the URL: **http://192.168.81.1:911**
This URL is only accessible from this port.

Once the following page is displayed, login using:

Username: admin
Password: 12pilot34



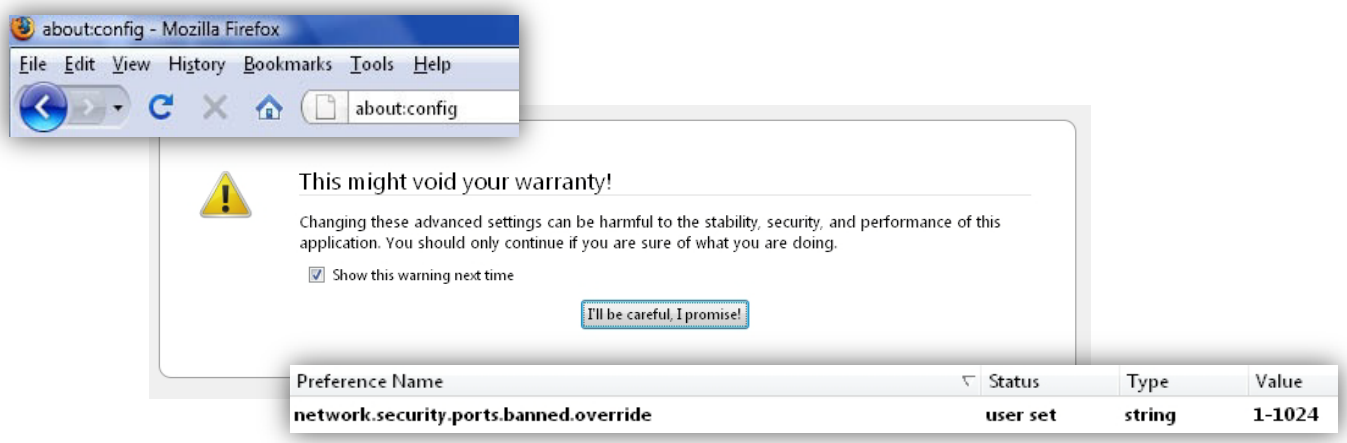
Once successfully logged into rescue mode, you will be able to perform the following tasks:  SSL Rescue, Reset Admin password, and reset User Accounts.


SSL Rescue
Press Execute to switch off SSL on the master GUI.
Execute
Reset Admin Password
Press Execute to change the Admin password to 123456.
Execute
Reset User Accounts
Press Execute to reset all user account settings and change the Admin password to 123456.
WARNING: The only user account that will exist after doing this is Admin!!!
Execute

# Troubleshooting:Mozilla FireFox Web Browser

If you have configured your STNS unit to be accessible via SSL, you can experience problems connecting through Firefox. You will need to modify your configuration in Firefox by performing the following tasks.

To override this type this in the address bar "about:config" and search for "network.security.ports.banned.override". This may or may not exist, if it doesn't, right click anywhere in the window and select new->string and use "network.security.ports.banned.override" as the name and the port number you need to connect to as the value. You can also select a range of ports by using "1-1024" as such a value or as a CSV style values such as "1024, 8080, 1-1000, 80".


about:config - Mozilla Firefox
File Edit View History Bookmarks Tools Help
about:config
This might void your warranty!
Changing these advanced settings can be harmful to the stability, security, and performance of this application. You should only continue if you are sure of what you are doing.
Show this warning next time
I'll be careful, I promise!
Preference Name
Status
Type
Value
network.security.ports.banned.override
user set
string
1-1024